GUILTY UNTIL PROVEN INNOCENT? A STUDY OF THE PROPRIETY AND LEGAL AUTHORITY FOR THE JUSTICE DEPARTMENT'S OPERATION CHOKE POINT

HEARING

BEFORE THE

SUBCOMMITTEE ON
REGULATORY REFORM,
COMMERCIAL AND ANTITRUST LAW

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

JULY 17, 2014

Serial No. 113–114

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

88–724 PDF WASHINGTON : 2014

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

BOB GOODLATTE, Virginia, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
STEVE CHABOT, Ohio
SPENCER BACHUS, Alabama
DARRELL E. ISSA, California
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
RAÚL LABRADOR, Idaho
BLAKE FARENTHOLD, Texas
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
RON DeSANTIS, Florida
JASON T. SMITH, Missouri
[Vacant]

JOHN CONYERS, JR., Michigan
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO R. PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
LUIS V. GUTIERREZ, Illinois
KAREN BASS, California
CEDRIC RICHMOND, Louisiana
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island

SHELLEY HUSBAND, *Chief of Staff & General Counsel*
PERRY APELBAUM, *Minority Staff Director & Chief Counsel*

SUBCOMMITTEE ON REGULATORY REFORM, COMMERCIAL AND ANTITRUST LAW

SPENCER BACHUS, Alabama, *Chairman*
BLAKE FARENTHOLD, Texas, *Vice-Chairman*

DARRELL E. ISSA, California
TOM MARINO, Pennsylvania
GEORGE HOLDING, North Carolina
DOUG COLLINS, Georgia
JASON T. SMITH, Missouri

HENRY C. "HANK" JOHNSON, JR., Georgia
SUZAN DelBENE, Washington
JOE GARCIA, Florida
HAKEEM JEFFRIES, New York
DAVID N. CICILLINE, Rhode Island

DANIEL FLORES, *Chief Counsel*

CONTENTS

JULY 17, 2014

Page

OPENING STATEMENTS

The Honorable Spencer Bachus, a Representative in Congress from the State of Alabama, and Chairman, Subcommittee on Regulatory Reform, Commercial and Antitrust Law 1
The Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Ranking Member, Subcommittee on Regulatory Reform, Commercial and Antitrust Law 2
The Honorable Bob Goodlatte, a Representative in Congress from the State of Virginia, and Chairman, Committee on the Judiciary 4

WITNESSES

The Honorable Stuart F. Delery, Assistant Attorney General, Civil Division, U.S. Department of Justice
Oral Testimony 17
Prepared Statement 20
Adam J. Levitin, Professor of Law, Georgetown University Law Center
Oral Testimony 122
Prepared Statement 125
Scott Talbott, Senior Vice President of Government Affairs, The Electronic Transaction Association
Oral Testimony 138
Prepared Statement 140
David H. Thompson, Managing Partner, Cooper & Kirk, PLLC
Oral Testimony 151
Prepared Statement 153
Peter Weinstock, Partner, Hunton & Williams LLP
Oral Testimony 168
Prepared Statement 171

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

Material submitted by the Honorable Spencer Bachus, a Representative in Congress from the State of Alabama, and Chairman, Subcommittee on Regulatory Reform, Commercial and Antitrust Law 8
Material submitted by the Honorable Doug Collins, a Representative in Congress from the State of Georgia, and Member, Subcommittee on Regulatory Reform, Commercial and Antitrust Law 27
Material submitted by the Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Ranking Member, Subcommittee on Regulatory Reform, Commercial and Antitrust Law 30
Material submitted by the Honorable Darrell E. Issa, a Representative in Congress from the State of California, and Member, Subcommittee on Regulatory Reform, Commercial and Antitrust Law 80

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement on behalf of the Virginia Bankers Association 187

Page

Prepared Statement of the Community Financial Services Association of America 191
Prepared Statement of the Independent Community Bankers of America (ICBA) 196
Prepared Statement of Marsha Jones, President, Third Party Payment Processors Association (TPPPA) 198
Questions for the Record submitted to Honorable Stuart F. Delery, Assistant Attorney General, Civil Division, U.S. Department of Justice 207
Questions for the Record submitted to Adam J. Levitin, Professor of Law, Georgetown University Law Center 209
Response to Questions for the Record from Scott Talbott, Senior Vice President of Government Affairs, The Electronic Transaction Association 210
Questions for the Record submitted to David H. Thompson, Managing Partner, Cooper & Kirk, PLLC 213

GUILTY UNTIL PROVEN INNOCENT? A STUDY OF THE PROPRIETY AND LEGAL AUTHORITY FOR THE JUSTICE DEPARTMENT'S OPERATION CHOKE POINT

THURSDAY, JULY 17, 2014

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON REGULATORY REFORM, COMMERCIAL AND ANTITRUST LAW
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to call, at 9:34 a.m., in room 2141, Rayburn House Office Building, the Honorable Spencer Bachus (Chairman of the Subcommittee) presiding.

Present: Representatives Bachus, Goodlatte, Issa, Marino, Holding, Collins, Smith of Missouri, Johnson, Garcia, and Jeffries.

Staff Present: (Majority) Daniel Huff, Majority Counsel; Ashley Lewis, Clerk; Justin Sok, Legislative Assistant to Rep. Smith of Missouri; Philip Swartzfager, Legislative Director to Rep. Bachus; Jaclyn Louis, Legislative Director to Rep. Marino; Ellen Dargie, Legislative Assistant to Rep. Issa; Jon Nabavi, Legislative Director to Rep. Holding; (Minority) Slade Bond, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. BACHUS. Good morning. The Subcommittee on Regulatory Reform, Commercial and Antitrust Law hearing will come to order.

Without objection, the Chair is authorized to declare recesses of the Committee at any time.

I am going to recognize myself for an opening statement.

Let me welcome everyone to today's oversight hearing on the Justice Department's Operation Choke Point program.

This Subcommittee has the duty of overseeing the Civil Division of the Justice Department, and today's hearing is part of fulfilling that important function.

By way of introduction, I approach this issue as not just a Subcommittee Chair on the Judiciary Committee, but as Chairman *emeritus* and former Chairman of the Financial Services Committee.

So this is a matter I have been following closely across both Committees for some time, as have Members on both sides of the aisle, including Congress Blaine Luetkemeyer from Missouri, who has done a lot of work and study on this program.

The intent of Operation Choke Point may have carried a purpose that we would all agree with, and that is to prevent financial fraud. However, my continued concern is that the program threatens to dry up legitimate sources of credit and financing.

Those left on the short end can often be the people who have the greatest difficulty in getting any credit at all. The program also can deny legitimate merchants access to financial networks they need to survive.

In this economy, the last thing we need is to make it harder for businesses to operate and employ workers, and by that I mean legitimate businesses.

Merchants that have been targeted by Operation Choke Point have not uniformly been called predatory lenders, as one might have presumed, but are a wide range of businesses, including coin dealers, firearms merchants, home-based charities, fireworks sellers, and even online dating services. That is a wide—very wide net. And one thing it immediately suggests is agency overreach.

To date, the Justice Department has served more than 50 administrative and investigative subpoenas on banks. Subpoenas are very expensive to comply with and can bring unwanted scrutiny.

So the natural reaction of a financial institution might be simply to sever a connection with a particular merchant and be done with it.

By forcing that kind of decision, a government agency is able to achieve a particular policy goal without touching the ball, to use a sports term. It strikes me that someone's due process rights are likely being violated.

We have heard the Department of Justice and the relevant bank regulators say that the goal of Operation Choke Point is not to eliminate businesses that might—that some might deem politically problematic.

However, after reviewing this issue, I am concerned that internal DoJ documents have revealed that, at a minimum, there have been an indifference to the risks that this policy poses to legitimate and lawful commerce.

Our witness today—in fact, we have a memo from Assistant Attorney General Delery that acknowledges—and let me quote from that—"the possibility that banks may stop doing business with legitimate lenders," but concluded—and I will quote again—"that solving that problem, if it exists, should be left to legitimate lenders themselves who can present sufficient information to banks to convince them that they are wholly legitimate."

That sounds like guilty until proven innocent.

Again, this is a program that I have followed with increasing concern. Last August I wrote Attorney General Eric Holder and FDIC Marty Gruenberg, asking both agencies to immediately stop any actions designed to pressure banks and payment processors to terminate business relationships with lawful lenders.

The fact that we are holding this hearing shows that there are many serious concerns that have yet to be satisfactorily addressed.

With that, let me again thank our witness for appearing today.

And let me yield to the Ranking Member for his opening statement.

Mr. JOHNSON. Thank you, Mr. Chairman.

Ordinary people, mostly minorities, mostly African-Americans, are being squeezed every day by the justice system.

They are sometimes prosecuted on shoddy evidence. They are coerced to accept unfair and unjustified plea bargains offered by prosecutors with unchecked and unbridled discretion.

And they are punished if they don't accept the plea and go to trial and get found guilty. They are threatened by these vindictive mandatory minimums, additional charges, and enhanced consecutive counts. So they plead guilty and still get a steep sentence.

They are serving these steep sentences in overcrowded prisons in a country with the largest known prison population in the world. And, for many, an incarceration practically becomes a life sentence due to the shortage of second chances for criminal offenders.

This is the state of our criminal justice system as it applies to ordinary folks, usually those from communities of color and without means. It is a system known as the new Jim Crow.

In the 4 years since Dodd-Frank, not one single person who facilitated or contributed to the greatest financial crisis since the Great Depression has been prosecuted. Not one person has been held accountable for this immeasurable hardship through a public trial in the criminal justice system.

Not one person has served as an example to those who would prey upon vulnerable members of society, including low-income minorities and the elderly, targeted with predatory loans which were then packaged and sold on Wall Street. And when they became nonperforming loans, these securities became worthless. Thus, the crash back in 2007.

And all of this taking place at a time when the United States Supreme Court, our activist Supreme Court, is bestowing corporations, rewarding corporations, with the rights that people have. Citizens United. The First Amendment right to freedom of speech has been conferred upon corporations.

And now with the Hobby Lobby decision, we have corporations with a religious right, a First Amendment right to freedom of religion to practice their religion.

But I know of no corporation that has gone to church and paid tithes, listened to the sermon, and went out and acted like a Christian.

I know of no corporation that has ever been to jail for operations on Wall Street or for—or Main Street. No corporation has ever been placed in jail. But, yet, they have the same rights that we have.

Earlier this week the Department of Justice announced a settlement with Citigroup based on its misrepresentations about the inherent risks of sub-prime mortgages and other egregious behavior.

This settlement includes a $4-billion penalty under the Financial Institutions Reform, Recovery and Enforcement Act, also known as FIRREA, F-I-R-R-E-A. Passed in the wake of the savings and loan crisis in the 1980's, FIRREA is a critical tool in uncovering and prosecuting illegal conduct.

In today's oversight hearing, this Subcommittee will consider the propriety and legality, the propriety and legality, of Operation Choke Point, which is the formal name for a series of investigations by the Justice Department's Civil Division under FIRREA of banks

that knowingly facilitate fraud that, in turn, affects the banks through unauthorized debits of consumers' accounts and other illegal activity.

Some of my Republican colleagues have disparaged these investigations under the theory that they enable the party in power to destroy businesses it favors without proof of wrongdoing.

But let's review the facts. The Justice Department has filed just one complaint against a financial institution as a result of Operation Choke Point. One.

In this lawsuit, the Justice Department alleged that Four Oaks Bank knowingly provided direct access to the financial system to parties engaged in defrauding consumers and illegal activities, such as a Ponzi scheme, illegal online gaming, and unlawful lending.

This bank not only permitted unlawful actors to directly access the financial system, it is alleged, it is also alleged that this bank allowed these parties to remove funds directly from consumers' accounts even after receiving thousands of complaints from consumers that these debits were unauthorized.

In fact, at one point, the bank stopped keeping track of consumer complaints altogether, illustrating its willingness to overlook fraudulent activity. In return for knowingly facilitating fraud, this bank received $850,000 in gross fees from a third-party processor.

Again, this is the only civil complaint filed by the Justice Department, and it was settled within days without going to trial and without any prosecution—criminal prosecution for actual fraud.

Instead of thanking the Justice Department for protecting untold consumers and the broader financial system from fraud, my Republican colleagues have hurled unfounded accusations, accusing public servants of abusing their power to destroy businesses that they simply dislike.

Although I am dumbfounded by this argument, one thing remains clear to me. For House Republicans, banks are still too big for regulations, too big for trial, too big to fail, to big for jail, too big to even investigate for fraud and money laundering, and too big to be held accountable for defrauding Americans.

I thank the Justice Department for fighting on behalf of consumers, and I encourage you to continue its investigations.

And I yield back.

Mr. BACHUS. Thank you, Mr. Johnson.

At this time I recognize the Chairman of the full Committee, Mr. Goodlatte, for his opening statement.

Mr. GOODLATTE. Mr. Chairman, thank you very much, and thank you for holding this hearing.

There is no dispute that consumer fraud is a real phenomenon. Approximately 10.8 percent of American adults fell victim to it in 2011. The Department of Justice should enforce the law vigorously on the villains who prey on our most vulnerable.

There is also no dispute that Operation Choke Point is cutting off some fraudster access to the banking system. The bipartisan concern is that there is an unacceptable level of collateral damage.

On this point, there appears to be a disconnect between statements from top officials and what is happening in practice. The of-

ficial line is that Operation Choke Point is targeting fraudsters, not the whole industry.

But the Committee has received numerous reports of banks severing relationships with law-abiding customers from legitimate industries that the Administration has designated "high risk."

For example, the Committee obtained a jarring account of a meeting between a senior FDIC regulator and a banker contemplating serving a payday lending client.

The official told the banker, "I don't like this product and I don't believe it has anyplace in our financial system. Your decision to move forward will result in an immediate unplanned audit of your entire bank."

This sounds more like strong-arming than law enforcement. It is naive to answer that the government is merely requiring banks to pay heightened attention to these clients, not disallowing them. That is not how the system works in practice.

Banks are highly regulated entities. They are at the mercy of their regulators, and that makes them risk-averse. To banks, high-risk merchants often are simply not worth the heightened scrutiny.

This thinking is so prevalent in the industry that it has been given a name: De-risking. The chairman of the Office of the Comptroller of the Currency lamented in a recent speech, "And whether or not DoJ intended it, it now seems clear that de-risking is occurring and wiping out legitimate business."

The Department of Justice can no longer claim this consequence is unintended. It allows Choke Point to continue without changes.

I also question the Justice Department's legal authority to pursue this dangerously overbroad program. The Financial Institutions Reform, Recovery and Enforcement Act is one of the few statutes that gives the Department authority to issue administrative, investigative subpoenas in the civil context.

Congress granted this authority in the wake of the savings and loan scandal to prevent fraud against banks. It applies to fraud affecting a Federally insured financial institution. Consumer fraud was not the focus.

Nevertheless, the Department of Justice relies on a recent district court case interpreting "affecting" broadly. In that case, though, the bank was perpetrating the fraud.

The district court, moreover, was careful to mention that the effects must be sufficiently direct and that there might come a point at which the effects on the bank are too attenuated.

Such is the case with Operation Choke Point. It targets banks neither as victims nor as perpetrators. Instead, it is manipulating banks whose payment processor clients have merchant clients who may or may not defraud their customers.

Accepting DoJ's legal authority requires one to believe that by "affecting" Congress meant to include fraud that was perpetrated not on banks and not even on their customers, but on the customers of their customers' customers.

Similarly, the reputational risk is not analogous. In the Department of Justice's precedent, the bank was accused of cheating its own customers, which obviously drives away customers who do not want to be their own bank's next victim.

By contrast, direct customers of banks targeted by Choke Point have no such concerns. Their bank is not defrauding them. The alleged problem is far removed from them and lies with the customers of their bank's clients' clients. In this setting, the prospect for reputational risk is highly attenuated, and DoJ's interpretation again appears highly strained.

Many of the concerns I have shared are bipartisan. A Democratic colleague told the Administration he wants to be sure we do not throw out the baby with the bathwater by shuttering lawful businesses. On March 27, 2013, 11 Democrats and 12 Republicans wrote banking regulators expressing a similar concern.

Good law enforcement is hard work and time-consuming. There are no shortcuts. Officers have to do the difficult work of identifying bad actors individually. They simply cannot profile entire industries.

I welcome Assistant Attorney General Delery, and I want to know what he makes of the devastating collateral damage to which some of our other participants will bear witness.

I also welcome all of our other witnesses and look forward to the discussion.

Thank you, Mr. Chairman.

Mr. BACHUS. Thank you.

Before I introduce Assistant Attorney General Delery—it is "Delery?"

Mr. DELERY. "Delery," Mr. Chairman.

Mr. BACHUS. "Delery." "Delery." Okay. There are some different pronunciations. They did a phonetic thing which I don't think is quite on it.

But before I make a formal introduction, I want to make two submissions for the record.

First, I ask unanimous consent to place in the record written testimony from Dr. Douglas Merrill, a Princeton Ph.D. and former Chief Information Officer for Google.

Mr. BACHUS. Google is a singing corporation, aren't they? Isn't that what they are? Maybe that is iTunes. They are not a singing corporation, are they? I guess not.

Mr. JOHNSON. Singing corporation?

Mr. BACHUS. You mentioned singing corporations. But anyway.

He specializes in applying radical innovation to solve hard problems, including the problem of credit access for the under bank.

He founded ZestFinance to use Google-style big-data math to provide credit to make smarter loans to under-served populations at lower rates.

His algorithm has enabled ZestFinance to slash default rates by half and offer up to 50 percent savings for borrowers. Then Operation Choke Point nearly destroyed his business.

He concludes that—and I quote—"More than 100,000 underbanked Americans overpaid tens of millions of dollars in fees because both ZestFinance and its partner, Spotloan, were limited by Choke Point."

Also like to submit for the record former FDIC Chairman Bill Isaac's letter. I ask unanimous consent to place in the record a letter from Bill Isaac, former Chairman of the FDIC, to the youngest member of the FDIC's board of directors in history—no. He is the

youngest member of the FDIC's board of directors in history, appointed by President Carter.

He explains that the Bank Secrecy Act and anti-money laundering provisions are—and again I quote—"are not intended to impose a duty on banks to ensure that their business customers are complying with every law in every State or that the businesses are treating customers fairly and delivering good value."

He also writes that, "Operation Choke Point is one of the most dangerous programs I have experienced in my 45 years of service as a bank regulator, bank attorney, consultant, and bank board member."

Is there any objection to this submission? Hearing none.

[The information referred to follows:]

Statement of
Douglas Merrill, Ph.D.
Founder/CEO, ZestFinance
Previous Chief Information Officer and Vice President of Engineering, Google

My name is Douglas Merrill, and I have been working on math and computer science problems in government and industry for more than 20 years. After completing my Ph.D. at Princeton, I became an Information Scientist at the RAND Corporation, a think tank focused on public policy. While there, I studied a variety of different topics ranging from military team development through to educational reform. RAND's view is that asking the right question can change the world, but that people often focus on the wrong point. After leaving RAND, I spent a few years at Price Waterhouse before moving to Charles Schwab as Senior Vice President of Common Infrastructure and Human Resources Strategy and Operations. Most recently, I was Chief Information Officer and Vice President of Engineering at Google. At Google, I was responsible for a large variety of tasks, including all internal technology; I also ran Google's innovative Initial Public Offering in 2004. My entire career has been driven by applying radical innovation to solve hard problems, including the problem of credit access for the underbanked.

In August of 2013, Federal agencies, including both the FDIC and Department of Justice, without discussion or public announcement, launched "Operation Choke Point". According to Michael Benardo of the FDIC, in a presentation to the FFIEC on September 17, 2013[1], Choke Point was designed to block illegal uses of the ACH network. However, it also targeted companies that are "Legitimate?" (sic), which includes domains as varied as ammunition sales, escort services, and "Pay Day Loans" (sic). At the same event, Joel Sweet from the DoJ commented on the "collateral benefits" of stopping "Internet Payday lending".

This amounts to blocking ACH usage by companies providing goods and services that the regulators did not approve of. ZestFinance was part of that collateral damage, even though our product was markedly better than alternatives—and legal in every state in which we offered the product. Operation Choke Point has resulted in almost half of my employees losing well-paying jobs with benefits. Regulation is critical for avoiding market failures and protecting customers; however, secret regulation that impacts legal businesses is inappropriate.

Overview

After leaving Google in 2008, I founded ZestFinance, with the goal of saving the underbanked billions of dollars by providing access to fair, transparent, and lower-cost credit. I got interested in this problem for a personal reason: My sister-in-law needed a new set of tires.

---

[1] Available at http://www.cvent.com/events/ffiec-information-technology-conference/agenda-d4978abdf411495996349c16dc2f11e3.aspx

Most of the people reading this testimony wouldn't blink an eye over buying a new set of tires. Even if we didn't have enough cash in a bank account to cover the cost, we could use a credit card to fund the purchase. But millions of Americans do not have access to even $300 in credit from a bank[2], and millions more would struggle to raise $2,000 on a month's notice from savings, credit, family and friends[3]. My sister-in-law, a single mother of three working her way through school with no other support, is one of the 25% Americans in this group.

She called me and we talked about her need for tires. Of course, I gave her the money to buy them. I was interested, though, in what her backup plan was – if I, say, had not answered my phone? She told me that she would just have taken out another payday loan. At the time, I didn't know what a payday loan was. I didn't know that there were approximately 25,000 payday loan stores in the US, which is more than Starbucks and McDonalds combined or that 10 million American households took out a payday loan in the past year[4], paying an aggregate of $7B in fees[5]. I know now that payday loans and other products from the "alternative financial system" are a key element of how millions of Americans make ends meet while waiting for the next paycheck to arrive.

Coming out of the call with my sister-in-law, I decided to ask the question that I had been taught at RAND—not "how do I eliminate high cost credit?"—but "how do I create a framework that allows innovation to transform the credit markets, thus lowering costs and increasing availability?". After learning more about the product, I concluded that there were real problems with how payday loans were designed:

- First, the loans were expensive in ways that are not captured solely by the stated rate. Payday loans typically charge at least $20-$25 for each $100 borrowed. Although $20 per $100 may not seem like a lot, the out-of-pocket cost can be extremely high if, as is usually the case, the borrower uses one payday loan to pay another or pays down only the interest. The median payday borrower pays almost $500 in fees.[6] At the extreme, the costs can be even higher. The top 10% of borrowers pay $1,000 in fees to borrow $350[7].

---

[2] Bhutta, Skiba, and Tobacman, 2012. "Payday Loan Choices and Consequences." Vanderbily Law and Economics Research Paper 12-30.
[3] Lusardi, Schneider and Tufano, 2011. "Financially Fragile Households: Evidence and Implications." Brooking Papers on Economic Activity 2011.1.
[4] Skiba and Tobacman, 2011. "Do Payday Loans Cause Bankruptcy". Available at http://ssrn.com/abstract=1266215
[5] The Pew Charitable Trusts, 2012. "Payday Lending in America: Who Borrows, Where They Borrow, and Why".
[6] The Pew Charitable Trusts, 2013. "Payday Lending in America: Report 2. How Borrowers Choose and Repay Payday Loans".
[7] Melzer, 2011. "The Real Costs of Credit Access: Evidence from the Payday Lending Market". The Quarterly Journal of Economics, 126.1.

- Second, they are effectively revolving lines of credit. Although the terms of a typical payday loan require the borrower to pay back the loan in a couple of weeks, this rarely happens. Most borrowers actually require several "different loans" in sequence to cover their debt needs, paying the fees over and over again without reducing the principal at all. This unfair structure results in a paralyzing balloon payment coming due at the end of a long sequence of payments.
- Third, the loans are opaque. Borrowers do not know how long it will take to pay off their loans and usually underestimate how long they will be in debt.

These three factors together – high fees, balloon payments, and unknown payment duration – cause second order problems for borrowers: Habitual borrowers have an increased risk of bankruptcy largely because so much of their income is devoted to paying payday fees. Borrowers do need access to credit that does not create additional financial uncertainty, but current payday products are not that.

Payday loans are so expensive not because lenders collude, or are generally evil, but rather because of high loss rates. This part of the math is not that complicated. Estimates vary, but about 50% of loans ultimately default[8], and as many 22% never make a single payment[9]. Rational lenders must charge fees that cover their losses, and, as a result, payday fees are very high. This burden falls disproportionately on people who pay back their loans, since, by definition, those that default do not pay the entire loan and the high fees. This "cross-subsidization" is another unfair aspect of the current payday loan market.

This problem, however, has a solution: Transform underwriting. Traditional underwriting relies on a simple equation that consumes a relatively small amount of data (as little as 50 pieces of information per application). This math has remained largely unchanged for decades. However, math and computer science have come a long way in the past few years, driven by places like Google. Google's computers use several hundred pieces of information and new math techniques to make web search, as we know it, possible.

ZestFinance applies Google-style math to the problem of underwriting, using tens of thousands of independent pieces of information to determine applicants' ability to repay and willingness to repay a loan. This approach relies on powerful computers executing very complex math, and is sometimes called "big data".

We at ZestFinance have proven that this approach works. ZestFinance's default rates are about half of others' in the industry. Equally importantly, ZestFinance offers installment loan products that are much different from payday loans. ZestFinance's loans are fully transparent – with no hidden fees – and for a fixed term

---

[8] Li, Mumford, and Tobias (2012). "A Bayesian analysis of payday loans and their regulation". Journal of Econometrics.
[9] Dobbie and Skiba (2011). "Information Asymmetries in Consumer Credit Markets". Vanderbilt University Law School, No. 11G05

that is long enough to give the customer a chance to repay with small installments. Regardless of the amount a borrower pays, every payment pays down both principal and interest. This structure results in far lower fees. Equally importantly, borrowers are not confused about how much they will pay.

Operation Choke Point

By 2013, ZestFinance was making loans directly to customers. In order to gain more data to improve our underwriting algorithms, the company was also providing technology support to unaffiliated lenders, including Spotloan. Together, ZestFinance and Spotloan employed 232 people across 17 states, paying millions of dollars in salary and benefits.

Last August, the Department of Justice launched Operation Choke Point. Although Operation Choke Point was intended to protect banks and their customers from illegal and fraudulent activity, Operation Choke Point also disrupted a number of legal businesses, including ZestFinance.

On August 28, 2013, Spotloan's sole ACH processor announced that, due to Operation Choke Point they would no longer process Spotloan payments, neither to fund borrowers' accounts nor to allow borrowers to make payments against their loans. They gave Spotloan 24 hours' notice. Not surprisingly, Spotloan could not respond in that timeframe, and, as a result, was unable to process any payments. Thousands of borrowers were unable to receive their loan funds and thousands more were cast in default through no fault of their own.

Spotloan was able to find another payment processor after several weeks. Then, on April 29, 2014, that alternative large ACH processor stopped processing Spotloan payments, as well.

Also, in the Choke Point period, funders for companies like ZestFinance and Spotloan became nervous. Since there had been little public discussion of what actions might fall afoul of Choke Point enforcement, the funders are not able to determine whether their money would simply vanish at a moment's notice. As a result, many funders simply stopped funding online loans or, even more severe, called in their current outstanding funds. Without such money, it became largely impossible to grow.

Although ZestFinance and Spotloan have each been able to stay afloat during this period, costs of doing business have spiked. Before Choke Point, an ACH transaction cost about $0.25. Today that same transaction costs between $3 and $7. And when a company like ZestFinance is even able to find funding to back its loans, the company will pay almost 50% more for the same funding it previously had.

These costs have to be offset somewhere and, sadly, that offset has been achieved through large layoffs. ZestFinance was forced to lay off 45% of its staff (about 21 people) and Spotloan laid off 85 people from its US staff (about 60%). Zest's layoffs cost the economy $4M per year in salary, and Spotloan's cost many millions more.

The reality is that the combination of funding loss, higher costs to operate the business, and job cuts have hurt the underbanked most of all: More than 100,000 underbanked Americans overpaid tens of millions of dollars in fees because both ZestFinance and Spotloan were limited by Choke Point.

Choke Point has also slowed down ZestFinance's innovation. This is the opposite of desirable public policy: Innovation is the way to improve credit access. Prior to Choke Point, the company was improving its underwriting algorithms, lowering default rates and cutting prices. In fact, ZestFinance had found a way to lower higher-quality borrowers' interest by hundreds of dollars per loan. Since Choke Point, an entire team of engineers and product managers has done nothing besides try to find and manage stable ACH processors, which means these highly skilled individuals are not working on improvements to help borrowers.

Summary

I founded ZestFinance to transform how the 60 million underbanked people in this country get credit. I wanted to ensure they had access to fair and transparent credit. ZestFinance innovated to find a way to offer up to 50% savings for borrowers. Equally importantly, both ZestFinance and Spotloan serve a real customer need by offering access to fair and transparent credit.

Illegal acts should be identified and prosecuted. But we should do so in a way that minimizes "collateral damage". People's livelihoods are not collateral damage. And we should not focus that damage on industries that we simply dislike.

Payday loans – and even far lower cost replacements like ZestFinance's installment loans – are expensive credit. There are people who find the existence of such credit to be evil. I do not agree: The underbanked deserve access to credit. In fact, ZestFinance's customers regularly reach out to thank us for giving them a safe bridge across their temporary financial crisis. I think it is inappropriate to deny credit to a large group of people because we – who are not in the situation – think the credit is too expensive. If lenders cannot cover their costs, they will not lend.

Innovation is the only hope for offering lower prices into underserved markets.

Innovations like those that we at ZestFinance are trying to accomplish.

We should use the administrative agencies' expertise to make innovations like ZestFinance's more welcomed and influential. I welcome a public discussion of how we can make credit more readily available to the underbanked, and how that credit should be priced.

I do not believe that Operation Choke Point has advanced that conversation.

July 16, 2014

Subcommittee on Regulatory Reform, Commercial and Antitrust Law,
Oversight Hearing on:
"Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point"
July 17, 2014 at 9:30 a.m.

Subcommittee Chairman: The Honorable Spencer Bachus
Ranking Member: The Honorable Hank Johnson

I regret that I will not be able to attend in person this incredibly important meeting of your Subcommittee. In lieu of attending in person, I will send separately written testimony expressing my views on Operation Choke Point. This testimony is substantially identical to the views I expressed under oath at a hearing by the Subcommittee on Financial Institutions and Consumer Credit of the House Financial Services Committee on July 15, 2014.

In addition to sending my previous testimony I would like to address some additional very important issues in this letter, pertaining particularly to the Bank Secrecy Act and Anti-Money Laundering laws (BSA/AML). The opinions I express are my own, and I do not purport to speak on behalf of my firm, FTI Consulting. In the interest of full disclosure, some of FTI's clients have an interest in the matters before the Subcommittee.

By way of background, I was appointed to the FDIC board of directors at age 34 by President Carter in 1978 and was named Chairman by President Reagan in 1981. I returned to the private sector at the end of 1985 after serving nearly two years beyond my six-year term at the FDIC. I also served during my term at the FDIC as Chairman of the Financial Institutions Examination Council (the coordinating body for the federal regulators of depository institutions) and as a member of the Basel Committee.

In my view, Operation Choke Point is one of the most dangerous programs I have experienced in my 45 years of service as a bank regulator, bank attorney and consultant, and bank board member. I fully support the bill introduced by Representative Luetkemeyer, HR 4986, to rein in this program.

Without legal authority and based on a political agenda, unelected officials at the Department of Justice (DOJ) are coordinating with some bank regulators to deny essential banking services to companies engaged in lawful business activities that some government officials don't like. Bankers are being cowed into compliance by an oppressive regulatory regime.

Perfectly lawful businesses are being denied access to essential banking services because they offer products or services unelected government officials do not like. This ought to alarm and frighten each of us irrespective of our ideology, party affiliation, or view of the particular products or services being cut off.

Operation Choke Point is a particularly egregious example of an un-Constitutional abuse of power. It is driving lawful businesses out of the banking system, denying them not

only loans but also deposit accounts, payments processing services, payroll accounts, and other services critical to operating any business.

I understand that some claim that Operation Choke Point does not impose any new burdens or responsibilities on banks or their customers – that banks are already responsible for knowing and policing their customers under the BSA/AML laws. The most obvious flaw in this fallacious assertion is that if it were correct, Operation Choke Point would not be needed.

The BSA/AML law has been around for decades. It began as a law intended to detect tax evasion and organized crime activity, including tracking drug money. It was expanded greatly after September 11, 2001 to include detecting flows of money possibly relating to terrorist activity. Banks are required to know their customers well enough to detect suspicious flows of funds that could signal illegal drug or terrorist activity and to report those suspicious funds flows to FinCEN. Banks are also supposed to detect transactions involving persons on the OFAC terrorist list and to reject those transactions.

If banks are lax in meeting these responsibilities their regulators can and do impose substantial penalties. Examiners from the banking agencies devote a good deal of attention to insuring the banks have proper BSA/AML controls in place and for the most part the industry is highly compliant.

BSA/AML is not intended to impose a duty on banks to ensure that their business customers are complying with every law in every state or that the businesses are treating their customers fairly and delivering good value. A bank will likely choose not to do business with customers who it believes are not treating people fairly or might be violating the law, but that is a judgment best left to the management and directors of individual banks to decide.

The Luetkemeyer bill would not relieve banks of any of their responsibilities under BSA/AML or any other law or regulation. Moreover, the bill states clearly that banks will retain the discretion to refuse to do business with any customer for any reason.

The indisputable truth is that Operation Choke Point is not about BSA/AML in any respect. The DOJ has decided to go after businesses that it and some other government agencies do not like – businesses such as home-based charities, fireworks and firearms distributors, short-term lenders, check cashers, pharmaceutical firms, life-time guarantees, surveillance equipment firms, and telemarketers. This is being done by the DOJ without any statutory authority and in fact in direct contravention of state and federal laws, including the Dodd-Frank Act.

We do not have to speculate about the strategy and motives behind Operation Choke Point, as they are set forth quite clearly in a September 9, 2013 memo written by Michael Blume, Director of the Consumer Protection Branch of the DOJ to Stuart Delery, Assistant Attorney General in the Civil Division of the DOJ, providing a six-month status report on Choke Point. Mr. Blume describes the strategies in these terms on page 14 of the report:

- ***We principally are pursuing civil, rather than criminal, investigations. Criminal investigations can take considerably longer to complete and generally require a more intensive investigation. Only if an investigation presents particularly egregious criminal conduct are we opening it as a criminal investigation.***

- ***We are targeting banks more than payment processors, and payment processors more than merchants. Any one case, whether against a bank, a processor, or a merchant, takes substantial time and attention from our team. Bank cases will deter other banks, thereby stopping the processing of transactions for fraudulent merchants and the processors with which they work. This may mean filing civil complaints or criminal cases against banks based on transactions with fraudulent merchants and/or processors – but not filing actions against the underlying fraudulent merchants or processors. This practice is not optimal and may present litigation risks. But it may be necessary to prevent the initiative from grinding to a halt due to resources used pursuing the merchants and processors.***

These words are chilling to anyone who has any regard for due process and the rule of law. Mr. Blume explains that the DOJ prefers using civil complaints rather than criminal complaints because the burden of proof is much lower and requires less investigation into the facts. And he explains that the DOJ is going after the banks who are not violating the law instead of the merchants who may be violating the law because the DOJ can do much more damage with much less effort by coercing the banks.

As for the claim by some that the DOJ is actually doing the banks a favor by protecting them from potential liability, Mr. Blume puts that notion to rest with the following passage from page 11 of his six-month report:

> ***The financial institutions we are investigating have not suffered any actual losses, but such actual losses are not necessary under FIRREA. There is only one case interpreting the phrase "affecting a financial institution" in the context of FIRREA, and that case supports our theory.***

Mr. Blume also addresses on page 10 of his report the collateral damage being done to lawful businesses that are being denied essential banking services such as deposit accounts, check clearing, and payroll processing:

> ***Although we recognize the possibility that banks may have therefore decided to stop doing business with legitimate lenders, we do not believe that such decisions should alter our investigative plans. Solving that problem – if it exists – should be left to the legitimate lenders themselves who can, through their own dealings with banks, present sufficient information to the banks to convince them that their business model and lending operations are wholly legitimate.***

Contemplate Mr. Blume's assumption that in our Constitutional republic a business is guilty until it proves itself innocent. There is no allegation of wrong doing by the business that can be disproved. The company is simply in a business that, while legal, has been determined "undesirable" and therefore "high risk" by the federal bureaucracy. This Orwellian result is frightening.

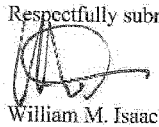
FinCEN and the federal banking agencies expect banking organizations that open and maintain accounts for money services businesses to apply the requirements of BSA, as they do with all accountholders, on a risk-assessed basis. As with any category of account-holder, there will be money services businesses that pose little risk of money laundering and those that pose a significant risk. It is essential that banking organizations neither define nor treat all money services businesses as posing the same level of risk. Operation Choke Point has led to blanket terminations of all firms within an industry without regard to the prescribed individualized risk assessments that banks have traditionally made with respect to their customers.

The Luetkemeyer bill is an extremely important step in reining in government agencies that are greatly overstepping their authority and breaching the Constitutional separation of powers among the three branches of government and between the states and federal government. While some of us may applaud the attack against payday lending, ammunition distributors, or home-based charities, we will likely take a different position when a new administration decides to attack activities more near and dear to our hearts.

Before closing, let me return to the claim some are making that Operation Choke Point does not require banks to do anything they are not already required to do under BSA/AML. This claim is demonstrably false, as anyone can readily see in reading Mr. Blume's six-month report. Moreover, if Operation Choke Point is not doing anything not already required by BSA/AML, there is no justification whatsoever for the continued operation of Choke Point. Nearly all banks were BSA/AML compliant long before Operation Choke Point was imposed by unelected government officials and will remain compliant long after Congress chokes off this disgraceful Operation.

I urge Congress to approve the Luetkemeyer bill without delay, as Operation Choke Point is doing severe and irreparable damage to firms engaged in lawful businesses approved by Congress and by state legislatures.

Respectfully submitted,



William M. Isaac

Mr. BACHUS. At this time I would like to introduce our first witness, Honorable Stuart Delery. Is that right? Good.

He was sworn in as Assistant Attorney General for the Civil Division on August 5, 2013, following confirmation by the U.S. Senate. He has led the division since March 2012.

As an Assistant Attorney General, he oversees the largest litigating division in the Department of Justice. Each year the Civil Division represents some 200 client agencies in approximately 50,000 different matters.

The Civil Division represents the United States in legal challenges to Congressional statutes, administrative policies, and Federal agency actions.

He joined the United States Department of Justice in January 2009 as chief of staff and counsel to the Deputy Attorney General and later served as Associate Deputy Attorney General. From August 2010 until March 2012, he served as senior counsel to the Attorney General.

Before joining the Department of Justice, Mr. Delery was a partner in the Washington, D.C., law firm of WilmerHale, where he was a member of the litigation department and the appellate and Supreme Court litigation practice group and a vice chair of the firm's securities department.

He graduated from Yale Law School and the University of Virginia. He clerked for Justice Sandra Day O'Connor and Justice Byron R. White of the U.S. Supreme Court and for Chief Judge Gerald—and how do you pronounce—"Tjoflat"?——

Mr. DELERY. "Tjoflat," Mr. Chairman.

Mr. BACHUS [continuing]. Of the U.S. Court of Appeals for the Eleventh Circuit.

So we welcome your testimony. And you are recognized for that purpose.

TESTIMONY OF THE HONORABLE STUART F. DELERY, ASSISTANT ATTORNEY GENERAL, CIVIL DIVISION, U.S. DEPARTMENT OF JUSTICE

Mr. DELERY. Thank you very much, Chairman Bachus, Ranking Member Johnson, and Members of the Subcommittee. Thank you for inviting me here today and for providing the Department of Justice the opportunity to describe our work designed to protect consumers from fraud perpetrated by certain merchants, third-party payment processors, and banks.

The Justice Department has made it a priority to fight consumer fraud of all kinds. Fraud against consumers comes in many forms, from telemarketing fraud to mortgage fraud, from lottery scams to predatory and deceptive online lending, and often strips our most vulnerable citizens of their savings and even their homes.

The Civil Division's consumer protection branch, along with the Criminal Division and the U.S. attorney's offices across the country, has worked for decades to protect the health, safety, and economic security of the American consumer.

Based on its years of experience in combatting fraudulent merchants and by following the flow of money from fraudulent transactions, the Department has learned that some banks and third-party payment processors, which are intermediaries between banks

and merchants, know that merchants are engaged in fraud and, yet, continue to process their transactions, in violation of Federal law.

As a result, in November 2012, our attorneys proposed a concentrated effort to pursue fraud committed by banks and payment processors as a complement to other consumer protection work.

This strategy aims both to hold accountable those banks and processors that violate the law and to prevent access to the banking system by fraudulent merchants, and this—this effort is sometimes referred to as Operation Choke Point.

One of our investigations now has been resolved, as was mentioned earlier, and provides a useful example of our efforts in this area.

In April, a Federal District Court in North Carolina entered a consent order and approved a settlement agreed to by the Department and Four Oaks Bank.

According to our complaint, Four Oaks allowed a third-party payment processor to facilitate payments for fraudulent merchants despite active and specific notice of fraud.

For example, Four Oaks received hundreds of notices from consumers' banks, including statements by account holders submitted under penalty of perjury, that the people whose accounts were being charged had not authorized debits from their accounts.

Four Oaks had evidence of efforts by merchants to conceal their true identities. Four Oaks also had evidence that more than a dozen merchants served by the payment processor had a return rate over 30 percent, a strong sign that the bank was facilitating repeated fraudulent withdrawals. And, indeed, one merchant had a return rate of over 70 percent.

According to our complaint, despite these and other signals of fraud, Four Oaks permitted the third-party payment processor to originate approximately $2.4 billion in debit transactions against consumers' bank accounts.

So as the Four Oaks case demonstrates, the Department's policy is to base its investigations on specific evidence of unlawful conduct.

Nevertheless, in recent months, we have become aware of reports suggesting that these efforts instead represented an attack on businesses engaged in lawful activity. And I thank you for the opportunity to clear up this misconception.

Our policy is to investigate specific unlawful conduct based on evidence that consumers are being defrauded, not to target whole industries or businesses acting lawfully, and to follow the facts wherever they lead us in accordance with the law, regardless of the type of business involved.

As with virtually all of our law enforcement work that touches on regulated industries, our work in this area includes communication with relevant regulatory agencies. Such communication is designed to ensure that we understand the industry at issue and that we have all the information we need to evaluate enforcement options in light of the evidence we uncover. That is nothing new.

So, for example, for many years, banking regulators have warned banks about the heightened risks to consumers associated with third-party payment processors.

In some of that guidance, FDIC has explained that, although many clients of payment processors are reputable merchants, an increasing number are not and should be considered high risk. And the FDIC has provided examples of high-risk merchants for purposes relevant to its regulatory mission.

The Department's mission, however, is to fight fraud. And we recognize that an entity simply doing business with a merchant considered high risk is not fraud.

So, in summary, our efforts to protect consumers by pursuing fraudulent banking activity are not focused on financial institutions that merely fail to live up to their regulatory obligations or that unwittingly process a transaction for a fraudulent merchant.

But when a bank either knows or is willfully ignorant to the fact that law-breaking merchants are taking money out of consumers' bank accounts without valid authorization and the bank continues to allow that to happen, the Department will not hesitate to enforce the law.

So thank you once again for the opportunity to appear before you today. And at this time, Mr. Chairman, I would be happy to answer any questions that you or the other Members of the Subcommittee may have.

[The prepared statement of Mr. Delery follows:]

Department of Justice

STATEMENT

OF

STUART F. DELERY
ASSISTANT ATTORNEY GENERAL
CIVIL DIVISION

BEFORE THE
SUBCOMMITTEE ON REGULATORY REFORM, COMMERCIAL AND ANTITRUST LAW
COMMITTEE ON JUDICIARY
U.S. HOUSE OF REPRESENTATIVES

FOR A HEARING RELATED TO

"OPERATION CHOKE POINT"

PRESENTED ON

JULY 17, 2014

Statement of Stuart F. Delery
Assistant Attorney General, Civil Division
Before the U.S. House of Representatives
Committee on Judiciary
Subcommittee on Regulatory Reform, Commercial and Antitrust Law
July 17, 2014

Chairman Bachus, Ranking Member Johnson, and Members of the Subcommittee, thank you for inviting me here and for providing the Department of Justice the opportunity to appear at today's hearing to describe our work designed to protect consumers from fraud perpetrated by certain merchants, third-party payment processors, and banks.

As the Attorney General has said, the Justice Department has made it a priority to fight consumer fraud of all kinds and to hold the perpetrators accountable. Consumer fraud comes in many forms—from telemarketing fraud to mortgage fraud, from lottery scams to predatory and deceptive on-line lending—and often strips our most vulnerable citizens of their savings and even their homes.

While there is seemingly no limit to the kinds of schemes that perpetrators of fraud invent, many of these schemes have one thing in common: they employ the banking system to take money from their victims. Once a fraudulent merchant can work his way into the banking system, he no longer has to convince unwitting consumers to hand over cash or mail a check. Instead, with the click of a button, he can debit their bank accounts and credit his own, repeatedly, without permission, and in violation of federal law—until somebody does something to stop it.

The Civil Division's Consumer Protection Branch—along with the Criminal Division and United States Attorney's Offices across the country—has worked for decades to protect the health, safety, and economic security of the American consumer. Based on its years of experience in combating fraudulent merchants, the Department, along with our law enforcement and regulatory partners, recognizes the critical role played by a limited number of third-party payment processors—intermediaries between banks and merchants—in allowing fraudulent merchants to gain access to our banking system and consumers' bank accounts. In some cases, these payment processors open bank accounts in their own names and, for a fee, use these accounts to conduct banking activities on behalf of their customers. While some customers are legitimate businesses, others are fraudulent merchants who either choose not to open their own bank accounts or cannot do so because banks will not do business with them. At the merchants' direction, the processor will initiate debit transactions against consumers' accounts and transmit the money to the fraudulent merchant.

Guided by the facts and the law, and by following the flow of money from fraudulent transactions, the Department has learned that some third-party payment

processors know their merchant clients are engaged in fraud and yet continue to process their transactions—in violation of federal law. Further, our experience in these cases has been that some banks, in violation of the law, either know about the fraud they are facilitating or are consciously choosing to look the other way. As a result, in November 2012, our attorneys proposed a concentrated effort to pursue the fraud committed by the banks and payment processors. This strategy aims both to hold accountable those banks and processors who violate the law and to prevent access to the banking system by the many fraudulent merchants who had come to rely on the conscious assistance of banks and processors in facilitating their schemes. This effort is sometimes referenced as Operation Chokepoint.

To begin the effort, using a variety of public and nonpublic sources, the Consumer Protection Branch assembled evidence of fraudulent activity by specific fraudulent merchants, payment processors, and banks. That information included statements of cooperating witnesses; tips and referrals from defrauded consumers and banks whose customers had been victimized; and evidence obtained during investigations of fraudulent merchants that identified third-party payment processors or banks participating in the merchants' unlawful conduct.

In addition, we obtained information from the Federal Reserve Bank of Atlanta concerning banks with abnormally high "return rates"—one possible indicator of potential fraud. "Return" or "chargeback" rates refer to the percentage of transactions that are reversed. In addition to "unauthorized" returns, which represent an explicit claim that a consumer did not authorize a debit in a transaction account, a high rate of "total" returns also indicates potential fraud. For example, returns due to insufficient funds may reflect consumers who had money taken from their accounts unexpectedly or repeatedly, without authorization. Returns due to a closed account may reflect consumers who were forced to close their bank accounts as a consequence of unauthorized debits.

Based on these and other sources, between February and August 2013, the Consumer Protection Branch issued civil subpoenas to specific banks, processors, and other entities for which the Department had specific evidence suggesting that those entities might be engaged in fraud or might have evidence of fraudulent conduct by others. We then reviewed the information provided in response to those subpoenas and, depending upon the nature of the evidence, we sought additional information, determined to pursue a civil or criminal investigation, or closed the file.

One of those investigations now has been resolved, and its resolution demonstrates exactly the type of troubling relationship between a bank and a set of perpetrators of fraud that gave rise to the Department's effort. On April 25, 2014, the U.S. District Court for the Eastern District of North Carolina entered a consent order and approved a settlement agreed to by the Department and Four Oaks Bank. According to the Department's complaint, Four Oaks allowed a third-party payment processor to facilitate payments for fraudulent merchants despite active and specific notice of the fraud, including:

- Four Oaks received hundreds of notices from consumers' banks—submitted under penalty of perjury—that the people whose accounts were being charged had not authorized the debits from their accounts.

- Four Oaks had evidence that more than a dozen merchants served by the payment processor had a "return rate" over 30 percent—a strong sign the bank was facilitating repeated fraudulent withdrawals. Indeed, one merchant had a return rate of over 70 percent.

- Four Oaks had evidence of efforts by merchants to conceal their true identities.

According to the Department's complaint, despite these and many other signals of fraud, Four Oaks permitted the third-party payment processor to originate approximately $2.4 billion in debit transactions against consumers' bank accounts, for which the bank received more than $850,000 in fees. As a result of the bank's actions, many American consumers were defrauded of their hard-earned savings.

The consent order, agreed to by Four Oaks and approved by the court, requires Four Oaks Bank to pay $1 million to the U.S. Treasury as a civil monetary penalty and to forfeit $200,000 to the U.S. Postal Inspection Service's Consumer Fraud Fund. It also obligates Four Oaks to take steps to prevent future consumer fraud.

As the Four Oaks Bank case demonstrates, the Department's policy is to base its investigations on specific evidence of unlawful conduct. Nevertheless, in recent months, we have become aware of reports suggesting that these efforts instead represented an attack on businesses engaged in lawful activity. I thank you for this opportunity to clear up this misconception. Our policy is to investigate specific conduct, based on evidence that consumers are being defrauded—not to target whole industries or businesses acting lawfully, and to follow the facts wherever they lead us, in accordance with the law, regardless of the type of business involved. We think this endeavor demonstrates the importance of holding financial institutions accountable when they participate in fraudulent activities, just as we hold accountable any other entity that engages in unlawful conduct.

As with virtually all of our law enforcement work that touches upon highly regulated industries, our work in this area includes communication with relevant regulatory agencies, here including the Federal Deposit Insurance Corporation (FDIC), the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the Federal Reserve Board. Such communication is designed to ensure that we understand the industry at issue, that our investigations do not unnecessarily or improperly frustrate regulatory efforts, and that we have all the information needed to evaluate the enforcement options available to address violations that our investigations uncover.

Federal law requires banks to "know their customers" in a variety of ways and to report instances of suspicious activity in order to prevent money laundering, consumer

fraud, and other illegal behavior. Banks are aware of these laws, and most have instituted programs to comply with these longstanding requirements. Indeed, it is because of these programs that many fraudulent merchants have difficulty engaging directly with banks and have come to rely on third-party payment processors for access to the banking system. Noting this trend, the FDIC—as part of its regulatory responsibilities—has warned banks about the heightened risks to consumers associated with third-party payment processors in its Guidance on Payment Processor Relationships first issued in 2008, and has explained that, "[a]lthough many clients of payment processors are reputable merchants, an increasing number are not and should be considered 'high risk.'" The FDIC has provided examples of "high-risk merchants" for purposes relevant to its regulatory mission. The Department's mission is to fight fraud, and we recognize that an entity's simply doing business with a merchant considered "high risk" is not fraud.

Indeed, we recognize that most of the businesses that use the banking system—even those in industries considered "high risk"—are not engaged in fraud, and we are dedicated to ensuring that our efforts to combat fraud do not discourage or inhibit the lawful conduct of honest merchants. While the Department's complaint against Four Oaks Bank demonstrates that many of the fraudulent merchants for which Four Oaks provided access to the banking system were engaged in illegal online short-term lending, we follow the facts where they lead us. The Department would only be interested in the conduct of an online short-term lender, or any merchant, to the extent that its conduct violates the law.

I thank you for this opportunity to reiterate what I and other Department officials have made clear on numerous occasions: that the Department is seeking to protect consumers from fraudulent practices in all industries and has no interest in pursuing or discouraging businesses engaged in lawful conduct. The Attorney General said this in a recent video posted publicly on the Department website. The Department has said this in response to Congressional inquiries. And the Department has said this many times to industry groups, including in a letter I wrote to the American Bankers Association and the Electronic Transaction Association.

Our efforts to protect consumers by pursuing fraudulent banking activity are not focused on financial institutions that merely fail to live up to their regulatory obligations or that unwittingly process a transaction for a fraudulent merchant. We are fighting fraud. When a bank either knows or is willfully ignorant to the fact that law-breaking merchants are taking money out of consumers' bank accounts without valid authorization, and the bank continues to allow that to happen, that is not just a concern for bank regulators. That is fraud, and it can result in true devastation for consumers. When any entity—whether it is a merchant, a third-party payment processor, or a bank—commits fraud against consumers, the Department will not hesitate to enforce the law. We will continue to pursue our mission to protect honest, hardworking Americans from those who put their financial security in peril.

Thank you, once again, for the opportunity to appear before you today. At this time, Mr. Chairman, I would be happy to address any questions you or Members of the Subcommittee may have.

Mr. BACHUS. Thank you very much.

First question will be Mr. Holding.

Mr. HOLDING. Thank you, Mr. Chairman.

You testified on Tuesday and, at that hearing, the FD—well, the—on Tuesday, the FDIC testified that they had authored a somewhat notorious high-risk activity list that predicates Operation Choke Point scrutiny.

You know, this is a somewhat dangerous list because it essentially tells banks that they shouldn't do business with certain industries, irrespective of the fact than an industry is operating entirely within the law, and most of these industries are legal under Federal, State, and local law. Some even have significant First Amendment protections.

So did the Department, the DoJ, conduct a review of whether any of these restrictions would violate the First Amendment rights of Americans? And, if they did not, why not?

Mr. DELERY. So, Congressman, the list that you are referring to, I believe, that was discussed by the FDIC on—at the hearing on Tuesday is a list that the FDIC prepared for its purposes.

As I said then, that was not something that the Department of Justice was involved in preparing. And whether a financial institution does business with a merchant that is in an industry on that list or any other list is not, under our policy, a basis for the investigations that we are talking about here.

Mr. HOLDING. Does the Department have its own definition of high-risk activity that would create liability under Operation Choke Point?

Mr. DELERY. Right. So that is not the basis for the policy or the actions that we are taking here.

Mr. HOLDING. But does the Department have their own definition, you know, of what seems to be somewhat of a term of art that is developing here?

Mr. DELERY. No. I don't believe so, Congressman.

The investigations that we are conducting are based on evidence of fraudulent conduct by particular institutions that are based on traditional law enforcement activities or investigative techniques.

So we are investigating institutions based on evidence——

Mr. HOLDING. So you don't pay any attention to that definition? So you don't use the FDIC's definition or list? That doesn't go into your calculus in making a decision—prosecutorial decision, Fourth Amendment decision?

Mr. DELERY. We are basing our investigations on evidence that we receive from various sources of actual fraudulent activity in a particular context. We are not looking at whole industries.

So the information may come from a referral from a bank whose customers have been victimized or complaints from the customers themselves or from investigations that we are conducting into fraudulent merchants.

Mr. HOLDING. Okay.

Mr. DELERY. So it is a standard series of investigative techniques.

Mr. HOLDING. Let's go to the funding.

The Department has a working capital fund used to support operations, and one part of that fund is known as the 3 percent fund

that allows the Department to, you know, retain 3 percent of affirmative civil recoveries.

You know, as this is a non-appropriated fund, there are no strings attached from Congress on how it is used and it inhibits oversight. You know, aside from an occasional question from Congress, the Department can use the money however it sees fit.

So, you know, these funds are utilized to hire attorneys, file additional enforcement actions. So I am concerned this is unaccountable and non-transparent and somewhat of a slush fund.

So I know you have been asked about this at another hearing. So, hopefully, you have had a chance to reflect and can answer it now.

How much money is currently held in the working capital fund? And how much money is utilized to hire attorneys? How many FTE does this support? And can you provide to the Committee an accounting for the last 5 years including the unobligated funds held?

Mr. DELERY. So, Congressman, that was a subject that came up at the hearing on Tuesday. We are looking into responding to similar questions, and we would be happy to take those back as well. I don't have the specific answers on that here today. We could certainly get back to the Committee on that.

You know—and, obviously, the Civil Division is not the only part of the Department that the 3 percent fund supports, and it only supports small and specified parts of—of the work that we do typically related to our affirmative—affirmative enforcement efforts.

Mr. HOLDING. Thank you.

Mr. Chairman, I yield back.

Mr. BACHUS. Thank you.

I am going to recognize Mr. Collins for a unanimous consent request and then the Ranking Member.

Mr. COLLINS. Thank you, Mr. Chairman.

And especially in light of the vote series and other things and with other schedules.

I have a letter here from TSYS, from Mr. Troy Woods, that I would like to enter into the record detailing concerns about Operation Choke Point, which highlight many of my concerns with this amazingly misguided program.

Mr. BACHUS. Hearing no objections, it is introduced.

[The information referred to follows:]

TSYS

One TSYS Way
Building C 4th Floor
Columbus, GA 31902
706 649 2104 tel

M. Troy Woods
President & COO, TSYS

July 14, 2014

Congressman Doug Collins
Cannon House Office Building
Room 513
Washington, DC 20515

Representative Collins:

I am writing to express TSYS' concerns regarding Operation Choke Point, a Department of Justice (DoJ) initiative that targets third-party payment processors and their financial institutions that process payments for businesses engaged in higher-risk, but legal, activities.

TSYS is in a unique position to assess the impact of Operation Choke Point. As a leading processor of credit card and debit card payments in the United States, TSYS deals with a wide variety of clients, including financial institutions of all sizes, community banks and credit unions, small- and mid-size businesses, large retailers, governments and millions of consumers. TSYS, as a third-party payments processor, operates an extensive behind-the-scenes infrastructure that facilitates the electronic exchange of funds between buyers and sellers in a manner that is fast, accurate, secure and compliant with applicable laws and regulations.

TSYS strongly believes that the present regulatory environment, which includes the prudential banking agencies, the Federal Trade Commission (FTC) as well as the Consumer Financial Protection Bureau, is sufficient to ensure that financial institutions and third-party payment processors implement sound risk management and mitigation, responsive fraud prevention and detection, and adequate consumer protections. Unfortunately, Operation Choke Point's broad scope has morphed the traditional fraud and risk-mitigation roles of these providers into law-enforcement roles and established a dangerous precedent.

TSYS is extremely concerned that Operation Choke Point gives financial institutions and third-party payment processors the untenable choice of either severing valuable and legal customer relationships or risking enforcement actions by DoJ and others. As noted in the Staff Report on Operation Choke Point issued by the U.S. House of Representatives Committee on Oversight and Government Reform, "Operation Choke Point has forced banks to terminate relationships with a wide variety of entirely lawful and legitimate merchants." Such actions have a direct impact on consumers.

Many payments industry groups are already working to strengthen practices and technologies aimed at protecting consumers from unscrupulous business practices. TSYS supports industry efforts to further strengthen internal controls or processes for entities that provide payment-processing services for customers engaged in higher-risk activities. Law enforcement, regulators and industry groups should work in partnership with common goals to reduce fraud and its impact on consumers.

Respectfully, DoJ should suspend Operation Choke Point and focus its resources directly or businesses that may be violating the law, rather than targeting financial institutions and third-party payment processors that provide payment services.

Thank you in advance for your consideration of these important matters.

Sincerely,

M. Troy Woods
President and COO

cc: G. Sanders Griffith, Sr. EVP and TSYS General Counsel
Deron R. Hicks, Associate TSYS General Counsel
Mark Pyke, Sr. EVP, President TSYS Merchant Services
Victoria Strayer, Sr. Director, TSYS Risk and Compliance
Robert Leebern, Esquire, Troutman Sanders
Scott Talbott, SVP, Government Affairs, Electronic Transactions Association

Mr. BACHUS. And the Ranking Member is now recognized.

Mr. JOHNSON. Mr. Chairman, I would like to be recognized for the—only for the purpose of introducing by unanimous consent for the record a letter from Howard Langer, a professor at the law school of the University of Pennsylvania and a founding Partner of Langer, Grogan & Diver, PC, which describes his work against Wachovia Bank, which paid full damages to 750,000 victims of approximately 130 mass market frauds.

And I would also like to tender for the record a letter from the Americans for Financial Reform, a coalition of several dozen consumer and civil rights groups, urging this Subcommittee to suppress efforts to ensure that banks and payment processors avoid facilitating illegal activity by complying with long-standing due diligence requirements to know their customers, monitor return rates, and be alert for suspicious activity; and, also, a—the written testimony of Lauren Saunders, who testified on behalf of the National Consumers Law Center in Tuesday's hearing on the Operation Choke Point in the Committee on Financial Services; and last, but not least, several guidance documents issued under the Bush Administration on high-risk merchants and payment processors.

I will tender these for the record.

Mr. BACHUS. Without objection, those materials are entered into the record.

[The information referred to follows:]

Americans for Financial Reform
1629 K St NW, 10th Floor, Washington, DC, 20006
202.466.1885

July 16, 2014

The Honorable Spencer Bachus
United States House of Representatives
2246 Rayburn Building
Washington, DC 20515

The Honorable Hank Johnson
United States House of Representatives
2240 Rayburn HOB
Washington, DC 20515

Re: Support Operation Choke Point and other efforts to fight payment fraud; oppose bills to curtail payment fraud work

Dear Chairman Bachus and Ranking Member Johnson:

Americans for Financial Reform and the undersigned community, consumer and civil rights groups urge you to support efforts to ensure that banks and payment processors avoid facilitating illegal activity by complying with longstanding due diligence requirements to know their customers, monitor return rates, and be alert for suspicious activity. Please oppose any bills to defund or weaken efforts to fight payment fraud or to insulate banks or payment processors that do not conduct appropriate due diligence or ignore red flags. We need every tool to fight data breaches, identity theft, scams, frauds, money laundering, and other illegal conduct.

Fraudsters Need Banks and Payment Processors to Access the Payment System

Many scams, frauds and illegal activity could not occur without access to the payment system. Banks and payment processors that originate payments play a critical role in enabling wrongdoers to debit victims' bank accounts and to move money around. Examples of unlawful activity that would not be possible without an originating bank include the following:

- A telemarketing scam defrauded seniors of $20 million by lying to them to get their bank account information.[1]
- A lead generator tricked people who applied for payday loans and used their bank account information to charge them $35 million for unwanted programs.[2]
- Bogus debt relief services scammed consumers out of $8 million and made their debt problems worse.[3]
- Wachovia Bank enabled $160 million in fraud by scammers targeting vulnerable seniors.[4]
- After an enforcement action against Wachovia, scammers moved their business to Zions Bank, which allowed it to continue despite spotting suspicious activity. For example, a

telemarketer calling a senior about a purported update to his health insurance card tricked him into revealing his bank account information.[5]

The FBI estimates that mass-marketing fraud schemes causes tens of billions of dollars of losses each year from millions of individuals and businesses,[6] and one study found that fraud drains $2.9 billion a year from the savings of senior citizens.[7] In addition, the data obtained in breaches like the recent Target, Michael's and P.F. Chang breaches would be useless without a bank to use that data to debit bank or credit cards accounts.

Banks are not always aware that they are being used to facilitate illegal activity. But when they choose profits in the face of blatant signs of illegality, they become an appropriate target for enforcement action. Indeed, if regulators do not take action against banks or payment processors facilitating illegal payments, they are left playing an impossible game of 'whack a mole' which makes it much too easy for fraudsters to get away with continuing to break the law, and processing institutions to continue to benefit from law-breaking.

Payment Fraud Hurts Everyone

Wrongdoers who access the payment system inflict harm on everyone. In addition to the *direct victims* of fraud, *the general public* spends millions of dollars on identity protection products and loses faith in the security of the payment system. *Retailers and online merchants* lose business if consumers are afraid to shop on their website or at their store. *Consumers' banks* bear the customer friction and the expense of dealing with unauthorized charges. *The fraudsters' banks and payment processors* may suffer regulatory or enforcement actions, lost customers, private lawsuits, and adverse publicity. *American security* is also put at risk when banks and processors that lack know-your-customer controls are used for money laundering for drug cartels, terrorist groups, and other criminals.

DOJ's Operation Choke Point

The Department of Justice's (DOJ) Operation Choke Point is aimed at banks that "choose to process transactions even though they know the transactions are fraudulent, or willfully ignore clear evidence of fraud."[8] The focus is on illegal conduct, not activity that DOJ deems immoral.

The first, and to date only, action that DOJ has brought as a result of Operation Choke Point is U.S. v. Four Oaks Fincorp, Inc., Four Oaks Bank & Trust Co. Four Oaks enabled payments for illegal and fraudulent payday loans; an illegal Ponzi scheme that resulted in an SEC enforcement action;[9] a money laundering operation for illegal internet gambling payments;[10] and a recidivist prepaid card marketing scam that made unauthorized debits for a bogus credit line.[11] DOJ charged that the bank ignored blatant red flags of illegality, including extremely high rates of payments returned as unauthorized; efforts to hide merchants' identities; offshore entities clearly violating U.S. laws; disregard for Bank Secrecy Act obligations by foreign entities; hundreds of

consumer complaints of fraud; and federal and state law violations, including warnings by NACHA and state attorneys general.

This type of disregard for know-your-customer requirements and the legality of payments is what led to last month's$8.9 billion penalty against BNP Paribas for concealing billions of dollars in transactions for clients in Sudan, Iran and Cuba,[12] and to a $1.92 billion penalty against HSBC for helping terrorists, Iran, and Mexican drug cartels launder money.[13] It is impossible to read the Four Oaks complaint without concluding that Operation Choke Point is essential work for which DOJ should be applauded, not criticized.[14] Calls to abandon Operation Choke Point are misguided and inappropriate.

Regulators Have Appropriately Warned Banks to be Aware of High-Risk Activities, But Banks Need Not Reject Legal Businesses

Separate from DOJ's Operation Choke Point, bank regulators have asked banks to be aware of higher-risk activities, defined as areas with a "higher incidence of consumer fraud or potentially illegal activities."[15] As with Operation Choke Point, the focus of bank regulators is on areas where fraud or illegal activity is prevalent. For example, telemarketing, credit repair services, and debt forgiveness programs have long been problematic areas plagued with fraud and deceptive conduct. Payday lending is a high-risk activity because it is completely unlawful in 15 states, is unlawful in nearly every other state if the lender lacks a state license, and, especially for online lending, often results in repeated debits that the consumer did not knowingly authorize.

Regulators have also made clear that banks that "properly manage these relationships and risks are neither prohibited nor discouraged" from providing services to lawful customers in high-risk areas.[16] Banks need only be aware of the potential for illegal activities; know their customers, including basic due diligence of high-risk businesses;[17] monitor payment return rates; and be alert for suspicious activity. These are not new obligations, but they are essential ones.

Some recent headlines have drawn sweeping, unsubstantiated conclusions based on individual bank account closures. Banks close accounts every day for a variety of reasons. The bank that closed the account of the adult entertainer, for example, has stated unequivocally that it was unrelated to either Operation Choke Point or any policy concerning her profession.[18] The same is true of a gun dealer who was cut off by its payment processor.[19]

Even the National Rifle Association has said:

> "[W]e have not substantiated that [anti-gun groups' efforts] are part of an overarching federal conspiracy to suppress lawful commerce in firearms and ammunition, or that the federal government has an official policy of using financial regulators to drive firearm or ammunition companies out of business."

Concerns by payday lenders that they are being rejected by some banks go back a decade or longer, long before the 2013 Operation Choke Point or the FDIC's 2011 guidance on payment

processing relationships. For example, in 2006, theFinancial Service Centers of America (FiSCA), which represents check cashers, money transmitters and payday lenders, testified:

> "For the past six years [since 2000] banks have been abandoning us - first in a trickle, then continuously accelerating so that now few banks are willing to service us ..."[20]

Anecdotes about a few closed accounts do not prove regulatory overreach. The bank could have seen signs of illegality; terminated a problematic processor that had both illegal and legal clients; terminated businesses that lacked adequate controls; made its own business decision to cut ties with payday lenders after the bank suffered adverse publicity from its own payday lending; or misunderstood inflammatory headlines and regulatory signals.

Some bank account closures may also be related to anti-money laundering (AML) and Bank Secrecy Act issues that are separate from whether the business is considered a high-risk business. Some payday lenders with state licenses are also check cashers and money transmitters, areas that require compliance with complicated but important AML rules. Recent money laundering settlements may have drawn more attention to those rules, andthe fact that Operation Choke Point is now in the news does not mean that every bank account closure is related.

Regulators are working to clear up any misconceptions created by overreaching headlines or exaggerated lobbyist claims, while also emphasizing the importance of work to prevent payment fraud. As FDIC Vice Chairman Thomas M. Hoenig said recently:

> [I]f the bank knows its customer, takes the necessary steps, has the right controls, then they ought to be able to engage with them.... But you need to do those things like BSA [compliance].... I do believe we have an obligation to say, "If you are following these rules, [you] have to then judge the risk that [you] are willing to take on." That's the process and I'm very comfortable with that.[21]

It is irresponsible and dangerous to halt scrutiny of banks and payment processors that close their eyes when they operate in areas with a high risk of illegality. There are thousands of banks in this country and plenty that will continue to handle high risk but lawful accounts. But the tens of billions of dollars that Americans lose to fraud every year and the harms permitted by money laundering are just too great to abandon all vigilance by banks and payment processors that are in a position to stop illegal activity.

Small Banks are Not a Target But May be Disproportionately At Risk

Banks large and small have received subpoenas and enforcement actions related to payment fraud. Butsmall banks may be disproportionately likely to process illegal payments or be harmed by payment fraud. Some fraudsters target small banks that lack the internal controls to spot suspicious activity or that (like Four Oaks Bank) need capital and look the other way in exchange for fee income. High risk activities without due diligence are also more dangerous to the safety and soundness of a small bank.

Moreover, more small banks are hurt by payment fraud than facilitate it. When the scammer's bank submits an unauthorized charge against a consumer's account, the consumer's bank incurs expenses to deal with the mess. Those costs can be substantial for small banks. When a consumer contests an unauthorized payment, the average bank cost for handling a return is $4.99. But for a small bank the cost is much higher: the average is over $100 and can be as high as $509.90, according to NACHA, the Electronic Payments Association.[22]

The disproportionate impact of payment fraud on smaller banks is a reason to *continue* efforts to stop illegal activity. It is not a reason to halt such efforts.

Conclusion

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. We urge you to support efforts to ensure that banks and payment processors do their part and to hold them accountable when they fail to comply with know-your-customer requirements, conduct due diligence on high-risk activities, or overlook obvious signs of illegality.

Yours very truly,

Americans for Financial Reform
Arizona Community Action Association
Arkansas Against Abusive Payday Lending
California Reinvestment Coalition
Center for Economic Integrity (Arizona)
Center for Responsible Lending
Coalition of Religious Communities
Consumer Federation of America
Consumer Action
Consumers Union
Kentucky Equal Justice Center
The Leadership Conference on Civil and Human Rights
National Association of Consumer Advocates
National Consumer Law Center (on behalf of its low income clients)
National Fair Housing Alliance
National People's Action
New Economy Project
NW Consumer Law Center
Public Citizen
Public Justice Center
South Carolina Appleseed Legal Justice Center
Texas Appleseed
U.S. PIRG
Virginia Citizens Consumer Council
Virginia Partnership to Encourage Responsible Lending
Virginia Poverty Law Center
Woodstock Institute

Cc: Members of the House Judiciary Committee Subcommittee on Regulatory Reform, Commercial and Antitrust Law

[1]*See* Federal Trade Comm'n, Press Release, "FTC Stops Mass Telemarketing Scam That Defrauded U.S. Seniors and Others Out of Millions of Dollars" (Mar. 31, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/03/ftc-stops-mass-telemarketing-scam-defrauded-us-seniors-others-out.

[2]*See* Federal Trade Comm'n, Press Release, "FTC Charges Marketers with Tricking People Who Applied for Payday Loans; Used Bank Account Information to Charge Consumers for Unwanted Programs" (Aug. 1, 2011), available at http://www.ftc.gov/news-events/press-releases/2011/08/ftc-charges-marketers-tricking-people-who-applied-payday-loans.

[3]*See* Federal Trade Comm'n, Press Release, "FTC Charges Operation with Selling Bogus Debt Relief Services; DebtPro 123 LLC Billed Consumers as Much as $10,000, But Did Little or Nothing to Settle Their Debts" (June 3, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/06/ftc-charges-operation-selling-bogus-debt-relief-services.

[4]*See* Charles Duhigg, "Bilking the Elderly, With a Corporate Assist," New York Times (May 20, 2007), available at http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=1&.

[5] Jessica Silver-Greenberg, New York Time, "Banks Seen as Aid in Fraud Against Older Consumers" (June 10, 2013), available at http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?pagewanted=all&_r=0.

[6] Federal Bureau of Investigation, International Mass-Marketing Fraud Working Group ,"Mass-Marketing Fraud: A Threat Assessment" (June 2010), available at http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment/mass-marketing-threat.

[7] The MetLife Study of Elder Financial Abuse (June 2011), available at https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf.

[8] The U.S. Department of Justice, "Holding Accountable Financial Institutions that Knowingly Participate in Consumer Fraud," The Justice Blog (May 7, 2014), available at http://blogs.justice.gov/main/archives/3651.

[9] S.E.C. v. Rex Ventures Group, LLC d/b/a Zeekrewards.com, et al., Civil Action 12-CV-519 (W.D.N.C.).

[10] United States v. Pokerstars, et al., 11-CV-02564 (S.D.N.Y.).

[11] Federal Trade Comm'n, Press Release, "FTC Sends Full Refunds to Consumers Duped by Marketers of Bogus '$10,000 Credit Line'" (May 12, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/05/ftc-sends-full-refunds-consumers-duped-marketers-bogus-10000.

[12] Danielle Douglass, "France's BNP Paribas to pay $8.9 billion to U.S. for sanctions violations," Washington Post (June 30, 2014), available at http://www.washingtonpost.com/business/economy/frances-bnp-paribas-to-pay-89-billion-to-us-for-money-laundering/2014/06/30/6d99d174-fc76-11e3-b1f4-8e77c632c07b_story.html.

[13] Ben Protess and Jessica Silver-Greenberg, "HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering," New York Times (Dec. 10, 2012), available at http://dealbook.nytimes.com/2012/12/10/hsbc-said-to-near-1-9-billion-settlement-over-money-laundering/.

[14] The complaint, which describes the fraud and the role of the bank and payment processor in detail, is available at http://www.courthousenews.com/2014/01/09/USvFourOaks.pdf. A summary of the key allegations is available at http://www.nclc.org/images/pdf/banking_and_payment_systems/letter-doj-payment-fraud.pdf.

[15] FDIC, Payment Processor Relationships, FIL-3-2012 (Jan. 31, 2012), available at http://www.fdic.gov/news/news/financial/2012/fil12003.html.

[16] FDIC, Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities, FIL-43-2013 (Sept. 27, 2013).

[17] For example, it is a simple matter to ask a payday lender in what state it lends and to show that it has licenses in those states.

[18] Dana Liebelson, "Is Obama Really Forcing Banks to Close Porn Stars' Accounts? No, Says Chase Insider," Huffington Post (May 8, 2014), available athttp://www.motherjones.com/politics/2014/05/operation-chokepoint-banks-porn-stars(quoting Chase source as saying: "This has nothing to do with Operation Choke Point ... we have no policy that would prohibit a consumer from having a checking account because of an affiliation with this industry. We routinely exit consumers for a variety of reasons. For privacy reasons we can't get into why.").

[19] Red Wing Ammunition Co. "isn't sure why he was cut off" by First Data, which stated: "First Data processes transactions for merchants selling firearms and ammunition, so long as they meet our longstanding credit/risk management policy requirements... These policies were implemented before the DOJ's Operation Choke Point and are unrelated." Jennifer Bjorhus, Star Tribune, "Federal antifraud initiative goes too far, banks say" (June 7, 2014), available at http://www.startribune.com/business/262167821.html.

[20] Gerald Goldman, General Counsel of FiSCA, "Summary Of speech before the U.S. House Committee on Financial Services, Subcommittee on Financial Institutions & Consumer Credit , Regarding Banking Services to MSBs (June 21, 2006), available at http://www.fisca.org/Content/NavigationMenu/GovernmentAffairs/TestimonySpeeches/FiSCAHearingOralStmtGoldman_6_21_06.pdf.

[21] Kate Davidson and Zachary Warmbrodt, Q&A: Thomas Hoenig, Politico Pro (June 13, 2014).

[22] NACHA-The Electronic Payments Association, "Improving ACH Network Quality by Reducing Exceptions" at 6 (Nov. 11, 2013). The NACHA study does not give an average cost for small banks, but the un-weighted average for all banks is $100.52, so the average for smaller banks is undoubtedly higher than that. The weighted average for all banks, taking into account each bank's volume, is $4.99.

Testimony of Lauren K. Saunders

Associate Director, National Consumer Law Center

On behalf of

Americans for Financial Reform
National Consumer Law Center (on behalf of its low income clients)
Center for Responsible Lending
Consumer Federation of America
U.S. PIRG

On
"Examining Regulatory Relief Proposals for Community Financial Institutions, Part II"

Before the Before the House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit

July 15, 2014

Chairman Capito, Ranking Member Meeks and Members of the subcommittee:

Thank you for inviting me to testify today on behalf of Americans for Financial Reform, the low income clients of the National Consumer Law Center, the Center for Responsible Lending, Consumer Federation of America, and U.S. PIRG.

I am here today to testify in support of Operation Choke Point and in opposition to H.R. 4986, which would undermine important efforts underway at the Department of Justice and banking regulators designed to ensure that banks do not facilitate illegal activity. I urge you to oppose any bills to weaken the ability of regulators to fight payment fraud or to insulate banks that do not comply with the law or that willfully ignore signs that they are enabling fraud, scams and other illegal conduct. We need every tool to fight data breaches, identity theft, scams, frauds, money laundering, and other illegal conduct.

I will first explain why vigilance by banks is so important to stop illegal activity. I will then discuss H.R. 4986 and will explain why it is inappropriate to immunize banks that fail to conduct due diligence or ignore red flags of illegality merely because the entity holds a state license, is registered as a money transmitter, or can find an attorney to say its conduct is legal.

In brief, merely holding a state license is no guarantee that an entity is acting legally, is not engaged in fraud or deceptive conduct, or is complying with laws designed to prevent money laundering or other illegal activity. Vigilance over money transmitters is essential to prevent fraudsters from concealing themselves and to prevent money laundering and financing for drug cartels and terrorism. Finally, fraudsters have lawyers who are willing to defend them, but the idea that a bank should be able to take a fraudster's attorney's word for the legality of payments and to ignore other signs of illegality is simply astounding.

I also join the testimony of Marcus Stanley of Americans for Financial Reform expressing serious concerns about the discussion draft of The Access to Affordable Mortgages Act of 2014, which would exempt "higher-risk mortgages" of $250,000 or under less that are held on the lender's balance sheet from new appraisal requirements included in the Dodd-Frank Act. The exemption would expose both consumers and financial institutions to the risks of an inflated appraisal.

Fraudsters Need Banks to Access the Payment System

Many scams, frauds and illegal activity could not occur without access to the consumer's bank or credit card accounts through the payment system. Banks that originate payments play a

critical role in enabling wrongdoers to debit victims' bank accounts and to move money around. Examples of unlawful activity that rely on an originating bank to process payments include the following:

- A $600 million internet pyramid and Ponzi scheme shut down by the SEC.[1]
- A telemarketing scam defrauded seniors of $20 million by lying to them to get their bank account information.[2]
- A lead generator tricked people who applied for payday loans and used their bank account information to charge them $35 million for unwanted programs.[3]
- Bogus debt relief services scammed consumers out of $8 million and made their debt problems worse.[4]
- Wachovia Bank enabled $160 million in fraud by scammers targeting vulnerable seniors.[5]
- After an enforcement action against Wachovia, scammers moved their business to Zions Bank, which allowed it to continue despite spotting suspicious activity. For example, a telemarketer calling a senior about a purported update to his health insurance card tricked him into revealing his bank account information.[6]
- Just last week, the FTC obtained a $6.2 million settlement against a payday loan broker that falsely promised to help consumers get loans and then used consumers' bank account information to make unauthorized withdrawals without their consent.[7]

The FBI estimates that mass-marketing fraud schemes cause tens of billions of dollars of losses each year from millions of individuals and businesses.[8] A MetLife study found that fraud drains $2.9 billion a year from the savings of senior citizens.[9] In addition, the data obtained in

breaches like the recent Target, Michael's and P.F. Chang breaches would be useless without a bank willing to use that data to debit bank or credit cards accounts.

Even when consumers voluntarily authorize a payment from their account to purchase a product or repay a loan, they may find that their account is repeatedly debited for fees or charges they did not authorize or additional products they did not buy. Just last month, a judge agreed with the FTC that a payday lender had deceived consumers about the cost of their loans by imposing undisclosed charges and inflated fees that were automatically deducted from their bank accounts.[10] Those deductions could not have been made without a bank to process the debits.

Banks are not expected to verify the legality of every payment they process, and they are not always aware that they are being used to facilitate illegal activity. But when they choose profits in the face of blatant signs of illegality, they become an appropriate target for enforcement action. Indeed, if regulators do not take action against banks facilitating illegal payments, they are left playing an impossible game of 'whack a mole' which makes it much too easy for fraudsters to get away with continuing to break the law, and processing institutions to continue to benefit from law-breaking.

Payment Fraud Hurts Everyone

Wrongdoers who access the payment system inflict harm on everyone. In addition to the direct victims of fraud:

- The general public spends millions of dollars on identity protection products and loses faith in the security of the payment system;
- Retailers and online merchants lose business if consumers are afraid to shop on their website or at their store;

- Consumers' banks bear the customer friction and the expense of dealing with unauthorized charges;
- The fraudsters' banks may suffer regulatory or enforcement actions, lost customers, private lawsuits, and adverse publicity; and
- American security is put at risk when banks and processors that lack know-your-customer controls are used for money laundering for drug cartels, terrorist groups, and other criminals.

DOJ's Operation Choke Point

The Department of Justice's (DOJ) Operation Choke Point is aimed at banks that "choose to process transactions even though they know the transactions are fraudulent, or willfully ignore clear evidence of fraud."[11] The focus is on illegal conduct, not activity that DOJ deems immoral.

The first, and to date only, action that DOJ has brought as a result of Operation Choke Point is U.S. v. Four Oaks Fincorp, Inc., Four Oaks Bank & Trust Co. Four Oaks enabled payments for illegal and fraudulent payday loans; an illegal Ponzi scheme that resulted in an SEC enforcement action;[12] a money laundering operation for illegal internet gambling payments;[13] and a prepaid card marketing scam that made unauthorized debits for a bogus credit line.[14] DOJ charged that the bank ignored blatant red flags of illegality, including extremely high rates of payments returned as unauthorized; efforts to hide merchants' identities; offshore entities clearly violating U.S. laws; disregard for Bank Secrecy Act obligations by foreign

entities; hundreds of consumer complaints of fraud; and federal and state law violations, including warnings by NACHA and state attorneys general.

This type of disregard for know-your-customer requirements and the legality of payments is what led to last month's$8.9 billion penalty against BNP Paribas for concealing billions of dollars in transactions for clients in Sudan, Iran and Cuba,[15] and to a $1.92 billion penalty against HSBC for helping terrorists, Iran, and Mexican drug cartels launder money.[16]

It is impossible to read the Four Oaks complaint without concluding that Operation Choke Point is essential work for which DOJ should be applauded, not criticized.[17] Calls to abandon Operation Choke Point are misguided and inappropriate.

Regulators Have Appropriately Warned Banks to be Aware of High-Risk Activities, but Banks Need Not Reject Legal Businesses

Separate from DOJ's Operation Choke Point, bank regulators have asked banks to be aware of higher-risk activities, defined as areas with a "higher incidence of consumer fraud or potentially illegal activities."[18] As with Operation Choke Point, the focus of bank regulators is on areas where fraud or illegal activity is prevalent. For example, telemarketing, credit repair services, and debt forgiveness programs have long been problematic areas plagued with fraud and deceptive conduct.

Payday lending is a high-risk activity because it is completely unlawful in 15 states, is unlawful in nearly every other state if the lender lacks a state license, and, especially for online

lending, often results in repeated debits that the consumer did not knowingly authorize. For example, the Four Oaks complaint described how many consumers were defrauded when they authorized a single payment from their bank account but found that the payday lenders debited their accounts repeatedly, without authorization, and would not stop.

Banks are permitted to provide services for entities that operate in high-risk areas as long as the bank undertakes due diligence to obtain reasonable assurances that the entity is operating legally. Regulators have made clear that banks that "properly manage these relationships and risks are neither prohibited nor discouraged" from providing services to lawful customers in high-risk areas.[19] Banks need only be aware of the potential for illegal activities; know their customers, including basic due diligence of high-risk businesses;[20] monitor payment return rates; and be alert for suspicious activity. These are not new obligations, but they are essential ones.

Some recent headlines have drawn sweeping, unsubstantiated conclusions based on individual bank account closures. Banks close accounts every day for a variety of reasons. The bank that closed the account of the adult entertainer, for example, has stated unequivocally that it was unrelated to either Operation Choke Point or any policy concerning her profession.[21] The same is true of a gun dealer who was cut off by its payment processor.[22]

Indeed, the National Rifle Association has said:

> "[W]e have not substantiated that [anti-gun groups' efforts] are part of an overarching federal conspiracy to suppress lawful commerce in firearms and ammunition, or that the

federal government has an official policy of using financial regulators to drive firearm or ammunition companies out of business."

Concerns by payday lenders that they are being rejected by some banks go back a decade or longer, long before the 2013 Operation Choke Point or the FDIC's 2011 guidance on payment processing relationships. For example, in 2006, the Financial Service Centers of America (FiSCA), which represents check cashers, money transmitters and payday lenders, testified:

> "For the past six years [since 2000] banks have been abandoning us - first in a trickle, then continuously accelerating so that now few banks are willing to service us ..."[23]

Anecdotes about a few closed accounts do not prove regulatory overreach. Banks close accounts for many reasons that may be unrelated to regulatory pressure or may be an appropriate response to regulatory guidance. Among other reasons, the bank could have:

- seen signs of illegality or fraud, even with a licensed entity, such as high rates of payments challenged as unauthorized;
- terminated a problematic payment processor that had both illegal and legal merchant clients;
- terminated businesses, like a payday lender that also does money transmitting, that lacked adequate controls to prevent money laundering;
- made the bank's own business decision to cut ties with payday lenders after the bank suffered adverse publicity from its own triple-digit deposit advance payday lending;

- eliminated unprofitable accounts in areas where the risks of illegality are not worth the effort to conduct due diligence; or
- misunderstood regulatory signals and inflammatory headlines.

Some bank account closures may be related to anti-money laundering (AML) and Bank Secrecy Act issues that are separate from whether the business is considered a high-risk business. Some payday lenders with state licenses are also check cashers and money transmitters, areas that require compliance with complicated but important AML rules. Recent money laundering settlements may have drawn more attention to those rules, and the fact that Operation Choke Point is now in the news does not mean that every bank account closure is related to it.

Regulators are working to clear up any misconceptions created by overreaching headlines or exaggerated lobbyist claims, while also emphasizing the importance of work to prevent payment fraud. As FDIC Vice Chairman Thomas M. Hoenig said recently:

> [I]f the bank knows its customer, takes the necessary steps, has the right controls, then they ought to be able to engage with them.... But you need to do those things like BSA [compliance].... I do believe we have an obligation to say, "If you are following these rules, [you] have to then judge the risk that [you] are willing to take on." That's the process and I'm very comfortable with that.[24]

It is irresponsible and dangerous to halt scrutiny of banks that close their eyes when they operate in areas with a high risk of illegality. There are thousands of banks in this country and

plenty that will continue to handle high risk but lawful accounts. But the tens of billions of dollars that Americans lose to fraud every year and the harms permitted by money laundering are just too great to abandon vigilance by banks that are in a position to stop illegal activity.

Small Banks are Not a Target But May be Disproportionately at Risk

Banks large and small have received subpoenas, enforcement actions and regulatory guidance related to payment fraud. But small banks may be disproportionately likely to process illegal payments and, even more so, are disproportionately likely to be harmed by payment fraud.

Some fraudsters target small banks that lack the internal controls to spot suspicious activity or that (like Four Oaks Bank) need additional revenue and are willing to look the other way in exchange for fee income. High risk activities without due diligence are especially dangerous to the safety and soundness of a smaller bank, particularly one that is undercapitalized.

On the flip side, more small banks are on the receiving end of illegal payments, not the originating end, and are themselves victims of payment fraud facilitated by other banks. When the scammer's bank submits an unauthorized charge against a consumer's account, the consumer's bank incurs expenses to resolve the issue.

Those costs can be substantial for small banks. When a consumer contests an unauthorized payment, the average bank cost for handling a return is $4.99. But for a small bank

the cost is much higher: the average is over $100 and can be as high as $509.90, according to NACHA, the Electronic Payments Association.[25]

The disproportionate impact of payment fraud on smaller banks is a reason to *continue* efforts to stop illegal activity. It is not a reason to halt such efforts.

H.R. 4986 Would Immunize Banks that Ignore Signs of Illegal Conduct and Would Undermine Essential Efforts to Fight Money Laundering, Payment Fraud and Illegal Activity

H.R. 4986 provides a highly problematic safe harbor for financial institutions that knowingly process payments for unlicensed merchants and fraudsters or willfully ignore signs of illegality. The bill also curtails the Department of Justice's ability to compel the production of important information necessary to determine if banks are facilitating illegal activity.

The bill forbids regulators from prohibiting, restricting or discouraging financial institutions from providing any product or service to an entity that:

- is licensed and authorized to offer such product or service;
- is registered as a money transmitting business; or
- has a "reasoned" legal opinion from a state-licensed attorney that purports to demonstrate the legality of the entity's business under applicable Federal and State law, tribal ordinances, tribal resolutions, or tribal-State compacts.

That is, regulators could not discourage financial institutions from providing processing services to an entity even if the institution observed alarmingly high levels of payments

challenged as unauthorized, was warned by federal or state law enforcement officials that the entity appeared to be engaged in fraudulent or deceptive conduct, knew that the entity had numerous court orders against it, or saw signs that the entity was attempting to conceal unlawful activity.

The fact that an entity holds a state license is no guarantee that it will not engage in unlawful activity. CashCall, Inc. for example, is a licensed lender in many states. But the CFPB has charged that CashCall, acting as a servicer and debt collector on payday loans made by Western Sky, debited consumer checking accounts for money they did not owe and continued debiting accounts even after Western Sky shut down its operations in response to numerous state enforcement actions and court orders.[26] CashCall has also faced prosecution by state attorneys general for its own lending activities, and California is in the process of revoking its license.

Yet, under H.R. 4986, regulators would not be permitted to advise financial institutions of the risks of processing payments for CashCall or from discouraging financial institutions from processing payments for entities facing similar government enforcement activity. The bill would not only permit continued debiting of consumer accounts for unlawful payments, it would also put financial institutions at risk of liability for chargebacks and legal action by consumers and others.

Similarly, even if an entity is registered as a money transmitting business, it could be violating the law or facilitating money laundering, consumer fraud, or other illegal activity. For example, Arizona Attorney General Tom Horne recently obtained a $94 million settlement with

Western Union, which was sending "blood wires" that permitted organized criminal cartels to smuggle money across the Arizona border. Attorney General Horne took the action to protect Arizonans from border violence, gun running, and human and narcotic smuggling along the southwest border.[27]

Under H.R. 4986, if a financial institution was serving a licensed money transmitter that was facilitating similar conduct, regulators could not discourage the activity or advise the financial institution of the risks.

Finally, virtually any criminal can find an attorney to defend its conduct, and sometimes the criminal hides the facts even from its own attorney. A legal opinion by an attorney that an activity is permissible should not absolve a financial institution from its obligation to conduct due diligence on of the third parties with which it does business and to keep its eyes open for suspicious activity. Financial institutions have clear guidance from regulators about how to manage relationships with third parties, including payments processors, and a letter from the third party's attorney cannot trump that guidance.

While this provision will aid any fraudster who has the ability to hire an attorney to write a letter on its behalf, it may have a particular impact on stopping regulators from advising financial institutions of the risks if they process payments for purportedly tribal entities that conduct activities off reservation in violation of state law. The Supreme Court's recent decision in the *Bay Mills* case should have made clear that tribes must obey state law when they act off reservation even if they have a license issued by a tribal entity to conduct business on tribal land.

A state "can shutter, quickly and permanently, an illegal casino," and the same is true of an illegal payday loan operation, by denying a license, obtaining an injunction, and even using the criminal law.[28] Yet even if the legality of unlicensed tribal payday lending is still up for debate, financial institutions that process electronic payments over the ACH system and remotely created checks over the check system provide warranties about the validity of those payments. If the payments turn out to be unlawful, the financial institution is on the hook to the consumer's bank, and a letter from the payday lender's attorney will not help. Regulators are only doing their duty to look out for the safety and soundness of financial institutions when they advise them of these high risk activities designed to evade state law.

H.R 4986 also curtails the Department of Justice's ability to issue subpoenas in connection with its investigations of financial fraud. A subpoena is merely a request for information. If a financial institution is potentially facilitating illegal activity, a subpoena is an important tool to determine the facts. Abusive practices, especially in cases of payments fraud, are hard to detect. For fraudsters, this is by design – the best scams are those that go undetected for as long as possible – so we cannot tie the hands of the regulators charged with enforcing the law. Regulators must have the ability to examine financial institutions, ensure that appropriate compliance procedures are in place, and when necessary, issue subpoenas, to detect fraud and investigate potential abuses.

Conclusion

Fighting payment fraud should not be controversial. Everyone benefits from efforts to stop illegal activity that relies on the payment system. I urge you to oppose H.R. 4986 and other

measures that would undermine efforts to ensure that banks comply with know-your-customer requirements, conduct due diligence on high-risk activities, and keep an eye out for signs of illegality. Everyone must do their part to protect the integrity of the payment system and to prevent illegal activity that harms millions of Americans, businesses and American security.

Thank you for inviting me to testify today. I would be happy to answer any questions.

---

[1] *See* SEC, Press Release, "SEC Shuts Down $600 Million Online Pyramid and Ponzi Scheme" (Aug. 17, 2012), available at http://www.sec.gov/News/PressRelease/Detail/PressRelease/1365171483920#.U8P2rpRdX9Z.

[2] *See* Federal Trade Comm'n, Press Release, "FTC Stops Mass Telemarketing Scam That Defrauded U.S. Seniors and Others Out of Millions of Dollars" (Mar. 31, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/03/ftc-stops-mass-telemarketing-scam-defrauded-us-seniors-others-out.

[3] *See* Federal Trade Comm'n, Press Release, "FTC Charges Marketers with Tricking People Who Applied for Payday Loans; Used Bank Account Information to Charge Consumers for Unwanted Programs" (Aug. 1, 2011), available at http://www.ftc.gov/news-events/press-releases/2011/08/ftc-charges-marketers-tricking-people-who-applied-payday-loans.

[4] *See* Federal Trade Comm'n, Press Release, "FTC Charges Operation with Selling Bogus Debt Relief Services; DebtPro 123 LLC Billed Consumers as Much as $10,000, But Did Little or Nothing to Settle Their Debts" (June 3, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/06/ftc-charges-operation-selling-bogus-debt-relief-services.

[5] *See* Charles Duhigg, "Bilking the Elderly, With a Corporate Assist," New York Times (May 20, 2007), available at http://www.nytimes.com/2007/05/20/business/20tele.html?pagewanted=all&_r=1&.

[6] Jessica Silver-Greenberg, New York Time, "Banks Seen as Aid in Fraud Against Older Consumers" (June 10, 2013), available at http://www.nytimes.com/2013/06/11/business/fraud-against-seniors-often-is-routed-through-banks.html?pagewanted=all&_r=0.

[7] See Federal Trade Comm'n, Press Release, "Phony Payday Loan Brokers Settle FTC Charges," (July 11, 2014) available at http://www.ftc.gov/news-events/press-releases/2014/07/phony-payday-loan-brokers-settle-ftc-charges.

[8] Federal Bureau of Investigation, International Mass-Marketing Fraud Working Group, "Mass-Marketing Fraud: A Threat Assessment" (June 2010), available at http://www.fbi.gov/stats-services/publications/mass-marketing-fraud-threat-assessment/mass-marketing-threat.

[9] The MetLife Study of Elder Financial Abuse (June 2011), available at https://www.metlife.com/assets/cao/mmi/publications/studies/2011/mmi-elder-financial-abuse.pdf.

[10] FTC, Press Release, "U.S. District Judge Finds that Payday Lender AMG Services Deceived Consumers by Imposing Undisclosed Charges and Inflated Fees" (June 4, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/06/us-district-judge-finds-payday-lender-amg-services-deceived.

[11] The U.S. Department of Justice, "Holding Accountable Financial Institutions that Knowingly Participate in Consumer Fraud," The Justice Blog (May 7, 2014), available at http://blogs.justice.gov/main/archives/3651.

[12] S.E.C. v. Rex Ventures Group, LLC d/b/a Zeekrewards.com, et al., Civil Action 12-CV-519 (W.D.N.C.).

[13] United States v. Pokerstars, et al., 11-CV-02564 (S.D.N.Y.).

[14] Federal Trade Comm'n, Press Release, "FTC Sends Full Refunds to Consumers Duped by Marketers of Bogus '$10,000 Credit Line'" (May 12, 2014), available at http://www.ftc.gov/news-events/press-releases/2014/05/ftc-sends-full-refunds-consumers-duped-marketers-bogus-10000.

[15] Danielle Douglass, "France's BNP Paribas to pay $8.9 billion to U.S. for sanctions violations," Washington Post (June 30, 2014), available at http://www.washingtonpost.com/business/economy/frances-bnp-paribas-to-pay-89-billion-to-us-for-money-laundering/2014/06/30/6d99d174-fc76-11e3-b1f4-8e77c632c07b_story.html.

[16] Ben Protess and Jessica Silver-Greenberg, "HSBC to Pay $1.92 Billion to Settle Charges of Money Laundering," New York Times (Dec. 10, 2012), available at http://dealbook.nytimes.com/2012/12/10/hsbc-said-to-near-1-9-billion-settlement-over-money-laundering/.

[17] The complaint, which describes the fraud and the role of the bank and payment processor in detail, is available at http://www.courthousenews.com/2014/01/09/USvFourOaks.pdf. A summary of the key allegations is available at http://www.nclc.org/images/pdf/banking_and_payment_systems/letter-doj-payment-fraud.pdf.

[18] FDIC, Payment Processor Relationships, FIL-3-2012 (Jan. 31, 2012), available at http://www.fdic.gov/news/news/financial/2012/fil12003.html.

[19] FDIC, Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities, FIL-43-2013 (Sept. 27, 2013).

[20] For example, it is a simple matter to ask a payday lender in what state it lends and to show that it has licenses in those states.

[21] Dana Liebelson, "Is Obama Really Forcing Banks to Close Porn Stars' Accounts? No, Says Chase Insider," Huffington Post (May 8, 2014), available at http://www.motheriones.com/politics/2014/05/operation-chokepoint-banks-porn-stars(quoting Chase source as saying: "This has nothing to do with Operation Choke Point ... we have no policy that would prohibit a consumer from having a checking account because of an affiliation with this industry. We routinely exit consumers for a variety of reasons. For privacy reasons we can't get into why.").

[22] Red Wing Ammunition Co. "isn't sure why he was cut off" by First Data, which stated: "First Data processes transactions for merchants selling firearms and ammunition, so long as they meet our longstanding credit/risk management
policy requirements... These policies were implemented before the DOJ's Operation Choke Point and are unrelated." Jennifer Bjorhus, Star Tribune, "Federal antifraud initiative goes too far, banks say" (June 7, 2014), available at http://www.startribune.com/business/262167821.html.

[23] Gerald Goldman, General Counsel of FiSCA, "Summary Of speech before the U.S. House Committee on Financial Services, Subcommittee on Financial Institutions & Consumer Credit , Regarding Banking Services to MSBs (June 21, 2006), available at
http://www.fisca.org/Content/NavigationMenu/GovernmentAffairs/TestimonySpeeches/FiSCAHearingOralStmtGoldman_6_21_06.pdf.

[24] Kate Davidson and Zachary Warmbrodt, Q&A: Thomas Hoenig, Politico Pro (June 13, 2014).

[25] NACHA-The Electronic Payments Association, "Improving ACH Network Quality by Reducing Exceptions" at 6 (Nov. 11, 2013). The NACHA study does not give an average cost for small banks, but the un-weighted average for all banks is $100.52, so the average for smaller banks is undoubtedly higher than that. The weighted average for all banks, taking into account each bank's volume, is $4.99.

[26] "CFPB Sues CashCall for Illegal Online Loan Servicing," Consumer Financial Protection Bureau (December 13, 2013) available at http://www.consumerfinance.gov/newsroom/cfpb-sues-cashcall-for-illegal-online-loan-servicing/

[27] Arizona Attorney General, "Western Union: CUTTING OFF THE ILLEGAL CASH FLOW: $94 Million Settlement to Aid Law Enforcement in Fighting Border Crime" (Feb. 3, 2014), available at https://www.azag.gov/border-security/western-union.

[28] Michigan V. Bay Mills Indian Community et al., 134 S.Ct. 2024, 2035 (2014).

LANGER GROGAN & DIVER P.C.
ATTORNEYS AT LAW

HOWARD LANGER
JOHN J. GROGAN*
EDWARD A. DIVER
IRV ACKELSBERG†
PETER LECKMAN‡

HOWARD LANGER
DIRECT DIAL (215) 320-5661
hlanger@langergrogan.com

1717 ARCH STREET
SUITE 4130
PHILADELPHIA, PA 19103

PHONE: 215-320-5660
FAX: 215-320-5703

GEOFFREY C. HAZARD,
OF COUNSEL

2263 CALIFORNIA STREET
SAN FRANCISCO, CA 94115
415-292-5535
ghazard@langergrogan.com

*ALSO ADMITTED IN NEW JERSE
†ALSO ADMITTED IN CALIFORNI
‡ADMITTED IN CALIFORNIA ON

July 15, 2014

The Honorable Spencer Bachus
United States House of Representatives
2246 Rayburn Building
Washington, DC 20515

The Honorable Hank Johnson
United States House of Representatives
2240 Rayburn HOB
Washington, DC 20515

Re: Hearing on Operation Chokepoint

Dear Chairman Bachus and Ranking Member Johnson:

I am Adjunct Professor of Law at the Law School of the University of Pennsylvania and the founding partner of Langer Grogan & Diver, P.C. I have spent the last eight years in cases involving banks, third party payment processors and mass market frauds. I was lead counsel in *Faloney v. Wachovia Bank* in which the bank paid full damages to some 750,000 victims of approximately 130 mass market frauds who had had money debited from their accounts. Wachovia had given the frauds access to the banking system through the use of several third party payment processors that Wachovia knew had taken on mass market frauds as customers. Over $150 million was recovered from Wachovia, representing the full amount taken from the victims' accounts. The victims could also file claims for overdraft fees that resulted from the funds having been taken from their accounts.

The behavior of Wachovia has been repeated over and again by other banks. Operation Chokepoint merely represents the continuation, albeit more intensively, of government actions seeking to curb banks and third party payment processors from enabling mass market fraud. This is no mere effort to recover from the deep pockets. In the cases I describe below the banks were fully on notice—actually aware—that they were enabling frauds through the accounts they serviced for third party payment processors.

Wachovia involved each of the elements at issue in Operation Chokepoint: a bank, third party payment processors, and multiple mass market frauds. Wachovia maintained the account of one payment processor, Payment Processing Center ("PPC"), even after its own due diligence report disclosed an:

> "article regarding a coupon scam in 1989 and 900-Line scam in 1991 involving Donald Hellinger [the principal of PPC]. The accused pled guilty to the coupon scam on October 24, 1989 for which he would face 8 years imprisonment…Information was also found regarding a suit filed by the FTC allegedly involving a company owned by Donald Hellinger…for deceptively promoting credit cards and other products via 900 numbers."

Each of the principals of PPC pled guilty to criminal charges growing out of their activities taken through Wachovia. Wachovia itself entered into a deferred prosecution agreement. Three other payment processors involved with Wachovia—Your Money Access, Suntasia, and Amerinet—were also subjects of government proceedings.

Following *Wachovia*, the Comptroller of the Currency brought an action against T-Bank of Dallas for engaging in the same conduct. T-Bank provided accounts to a third party payment processor known as Giact Systems, which like PPC, had many mass market frauds as customers. As in the case of Wachovia, T-Bank was required to make full restitution to all the victims whose accounts had been raided by the frauds. See, http://www.occ.gov/static/enforcement-actions/ea2010-067.pdf

The Justice Department, in a joint action with banking regulators, brought an action against the First Bank of Delaware for engaging in identical activity. It opened accounts for a series of third party processors all of which engaged in servicing mass market frauds. These included Landmark Clearing, Inc., Automated Electronic Checking, Inc., Check Site, Inc., and Check 21.com, LLC. See, Complaint, *United States v. First Bank of Delaware*, Civil Action No. 12-6500 (E.D. Pa. 11/19/12) The government was unable to obtain full restitution for the victims of the frauds that had raided victims' account through First Bank of Delaware because the bank lacked sufficient assets. Its charter was revoked. *See,* http://www.fincen.gov/news_room/nr/html/20121119.html.

The Committee is familiar with the successful Justice Department action against *Four Oaks* which also enabled frauds through a third party payment processor.

My own firm has brought an action against Zions First National Bank a large bank located in Utah. Zions used a wholly owned third party processor for which it opened accounts in order to bank accounts that it acknowledged it would never have accepted directly. Not surprisingly 49% of revenue of the payment processor, known as Modern Payments ("MP/ND"), was derived from mass market frauds ultimately shut down by the FTC or the Justice Department. The type of businesses Modern Payments serviced is described in *F.T.C. v. NHS Sys., Inc.*, 936 F. Supp. 2d 520, 526 (E.D. Pa. 2013). In the case against Zions, the district court found that the plaintiffs had pled facts establishing Zions' knowledge of the fraud of the entities it was servicing:

> Reyes has sufficiently pleaded his § 1962(c) claims against the Zions Defendants. He alleges Zions Bank and MP/ND each serve independent and crucial roles in conducting an enterprise with the common purpose of earning fees for facilitating fraudulent telemarketing schemes. ...In alleging the Zions Defendants knew the transactions were fraudulent, Reyes pleads facts showing Zions Bank and MP/ND were aware of several blatant indications of fraud, including NHS's and related telemarketers' staggeringly high rates of ACH returns, and in particular, rates of return for lack of authorization. Reyes asserts Zions Bank discussed the high return rates with MP/ND, and MP/ND communicated frequently with the allegedly fraudulent telemarketers about their return rates. Reyes also alleges Zions Bank and MP/ND received notification from another bank they were violating NACHA's rule prohibiting ACH TEL transactions for outbound telemarketing...

Reyes v. Zion First Nat. Bank, CIV.A. 10-345, 2012 WL 947139 (E.D. Pa. Mar. 21, 2012)

The court subsequently denied class certification in the *Zions* action and the Third Circuit has accepted interlocutory review of the decision. If *Zions* is successful in sustaining the district court's decision on appeal, cases like those brought under Operation Chokepoint becomes all the more important since victims otherwise would lack a means of redress. The AARP, the Consumer Federation of America, The National Consumer Law Center, Senators Casey, Blumenthal and Markey and others have filed friend-of-court briefs supporting reversal of the denial of class certification in *Zions*.

The cases discussed above underscore the importance of Operation Chokepoint. The various frauds migrated from bank to bank. The very same persons who operated the NHS fraud through Zions had operated a similar fraud through Wachovia. Several of the frauds involved in the T-Bank and First Bank of Delaware cases had simply migrated to Zions. Had the banks engaged in the most rudimentary due diligence they would have turned up these migrating frauds. Wachovia and Zions both obtained the fraudulent customers through what are known as account brokers. The account broker who brought PPC to Wachovia testified that four other banks had refused to open accounts for PPC before Wachovia accepted it. The perpetrator of the NHS fraud testified that he was approached by an account broker who brought his account to Zions within twenty-four hours of losing his prior access to the banking system, through a court order freezing PPC's accounts at Wachovia. The banks engaged in servicing these frauds did not innocently stumble into the business when a new depositor simply walked through the doors and asked to open an account.

Nor is the Department of Justice requiring anything new of banks. For years the Comptroller of the Currency has made it clear that banks had a special obligation to undertake particularly careful due diligence in taking on third party processors accounts. This is set out in detail in the government's complaint against *Four Oaks*, so I do not repeat it here. The fact that the government has stepped up enforcement should be endorsed by Congress, not criticized. It is only when banks follow the regulatory requirements of due diligence in accepting accounts that such mass fraud will stop. The frauds will lose access to the victims' bank accounts.

It is not surprising that the recently formed association of third party payment processors urges action against Operation Chokepoint. The many actions I have described above confirm the warnings that the banking regulators have been providing to banks that accepting accounts of third party payment processors are fraught with risks. At least eleven different third party payment processors are identified in the complaints described above as having served as conduits for hundreds of millions of dollars in mass market fraud.

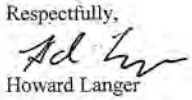
The representatives of the payday lending industry also urge that Operation Chokepoint be shut down. As the Committee knows, payday lending is outlawed in many states, like my own state, Pennsylvania. Payday lenders charge exorbitant interest rates, often exceeding 100%, and only the most desperate avail themselves of such usurious loans. But putting that aside that most basic moral concern, experience in the above cases shows that payday lending has been associated with mass market frauds. Certain of the frauds at issue in the *Zions* matter were payday loan referral cites which obtained victims' bank account information and used the information to raid victims' accounts through the electronic debit system. Worse, it is common for such frauds to exchange these illicitly compiled lists with each other. A so- called "legitimate" payday lender and payday loan referral site, Money Mutual, has a small print "privacy" policy on its website which makes explicit that it may sell the banking information it obtains to telemarketers:

> If you choose to provide personal information, … We reserve the right to share, rent, sell or otherwise disclose your information with/to third parties in accordance with applicable laws and as described herein. These third party businesses may include, but are not limited to: providers of direct marketing services and applications, including …; e-mail marketers; … and telemarketers. Information collected by us may be added to our databases and used for future instant messaging, telemarketing….

It is difficult to understand why anyone, let alone public servants, would undertake any action on behalf of such entities to curb the very type of enforcement activity citizens expect from government. I hope that the Committee will find from the above that there is good reason for the Department of Justice to pursue the course undertaken in Operation Chokepoint.

While I will be teaching abroad from August 3 through August 18, the committee should not hesitate to contact me should it want to explore the matters discussed above.

Respectfully,



Howard Langer

cc: Members of the House Judiciary Committee
Subcommittee on Regulatory Reform,
Commercial and Antitrust Law

Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC BULLETIN 2006-39

Subject: Automated Clearing House Activities
Date: September 1, 2006

To: Chief Executive Officers, Chief Risk Officers, and Compliance Officers of All NationalBanks, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

Description: Risk Management Guidance

As of October 30, 2013, this guidance applies to federal savings associations in addition to national banks.*

Table of Contents

Purpose
Scope
Background
Discussion
- ACH Risk Management Program
- Credit Risk
- High-Risk Activities
- Compliance Risk
- Third-Party Service Providers
- Direct Access to the ACH Operator
- Transaction Risk
- Information Technology

Conclusion
Additional Information

Purpose

This bulletin provides guidance for national banks and examiners on managing the risks of automated clearing house (ACH) activity. National banks may be exposed to a variety of risks when originating, receiving, or processing ACH transactions, or outsourcing these activities to a third party. This bulletin outlines the key components of an effective ACH risk management program. Each bank should use this guidance to develop an ACH risk management program that reflects the nature and complexity of the bank's activities.

This bulletin supplements guidance on ACH activities contained in the *FFIEC IT Examination Handbook on Retail Payment Systems*, [1] dated March 2004, and National Automated Clearinghouse Operating Rules [2] and replaces OCC Bulletin 2002-2 (ACH Transactions Involving the Internet).

Scope

This guidance applies to

- Banks acting as originating depository financial institutions (ODFIs),

- Banks acting as receiving depository financial institutions (RDFIs),
- Banks considering these activities, and
- Third-party service providers acting on behalf of an ODFI or RDFI.

Background

Advances in technology have brought about significant changes in the nature and volume of ACH activity. The growth in ACH volume results from fundamental changes in payment methods used by consumers and businesses. Recently, the OCC has seen banks engage in new ACH activities without enhancing existing risk management systems and controls. Failure to implement appropriate controls for these activities is an unsafe and unsound practice and can result in increased credit, compliance, reputation, strategic,and transaction risks, and in some cases, deterioration in the bank's condition.

ACH origination volume has increased as consumers and businesses look for more cost-effective and convenient payment alternatives. The most pronounced growth in ACH transactions over the last several years has been for nonrecurring payments. Consumers may initiate such payments over the telephone, on the Internet, or simply by writing a check that is converted to an ACH transaction. Some common nonrecurring payment types include accounts receivable conversion (ARC) [3], point-of-purchase (POP), Internet-initiated (WEB), telephone-initiated (TEL), and re-presented check (RCK) entries.

In addition to new and evolving types of ACH transactions, there are new participants in the ACH network, including certain merchants and third parties known as third-party senders. Whereas a bank is a client of a traditional third-party service provider (often called an ACH vendor), the merchant is the customer of a third-party sender (often called an originator aggregator or merchant processor) and the third-party sender is a customer of the bank. When a third-party sender is interposed between the bank and the originator, there is no contractual agreement between the bank and originator. A bank should be aware of the distinct risks arising from relationships with third-party senders. Although third-party senders are bank customers, they require oversight by bank management. Guidance on managing third-party senders can be found in the *Third Party Senders* section of this document.

Discussion

ACH Risk Management Program

Banks that participate in the ACH network, as well as their service providers, should have in place systems and controls to mitigate the risks associated with ACH activities. A strong risk management program begins with clearly defined objectives, a well-developed business strategy, and clear risk parameters. Both the board of directors and management are responsible for ensuring that the ACH program does not expose the bank to excessive risk. The board's role is to establish the bank's overall business strategy and risk limits for the ACH program and to oversee management's implementation of the program. Bank management is responsible for establishing effective risk management systems and controls and regularly reporting to the board on the results of the ACH program.

The bank's ACH program should include an ongoing process that evaluates whether ACH activities are conducted within the risk parameters established by the board of directors. This process should also determine whether existing policies, procedures, and controls effectively address all aspects of the bank's ACH activities.

Risk Management Systems and Controls

The systems and controls needed for an effective ACH risk management program include written policies and procedures, strong internal controls, and a risk-based audit program. The depth and breadth of a bank's ACH policies and procedures will depend on the scope and complexity of the ACH activities. Adequate policies and procedures generally include the following basic components:

- A summary of the ACH program's objectives and its role within the bank's strategic plan;
- Board-approved risk tolerances that outline the types of activities the bank may conduct and the types of businesses approved for ACH transactions;
- Clearly defined duties and responsibilities that ensure strong internal controls over transactions;

- An ACH credit-risk management program; and
- An effective vendor management program, including a due diligence process for selecting third-party service providers, and an oversight process for monitoring them.

Reporting to the Board of Directors

To oversee management's execution of the ACH program effectively, the board of directors, or a committee thereof, should receive periodic reports that allow the board to determine whether ACH activities remain within board-established risk parameters and are achieving expected financial results. Such reports generally include:

- Metrics and trend analyses on ACH volume, returns, operational losses, and transaction types, with explanations for variances from prior reports;
- Metrics and trend analyses related to the composition of the bank's portfolio of originators and, as applicable, third-party senders;
- Capital adequacy relative to the volume of ACH activity and the level of risk associated with originators;
- The percentage of the deposit base that is linked to ACH origination activity;
- A summary of return rates by originator, and, as applicable, third-party senders; [4]
- Unauthorized returns that exceed board-established thresholds;
- Notices of potential and actual rules violations and fines by NACHA;
- Financial reports on profitability of the ACH function as a cost center; and
- Risk management reports, including a comparison of actual performance to approved risk parameters.

Audit

The depth and breadth of a bank's ACH audit program will depend on the volume and complexity of its ACH operations. The OCC has seen several cases in which a bank's ACH audit program was not enhanced or strengthened to cover new or expanded products and services, including high-risk activities. Common deficiencies include inadequate audit coverage, inexperienced audit staff, and a lack of appropriate auditor training.

When establishing the ACH audit scope, auditors should consider issues such as growth in transaction volume, new products and services, new ACH systems, underwriting policies and customer due diligence (CDD) policies and practices, and customers' online access to the ACH network. Bank management should also ensure that periodic audits of third-party service providers and third-party senders are performed. The audit should also check for completion of the annual National Automated Clearing House Association (NACHA) Rules Compliance Audit (Rules Audit) by the bank or third-party service provider. The Rules Audit, however, is only one element of an effective ACH audit program and is not a substitute for a comprehensive, risk-based audit.

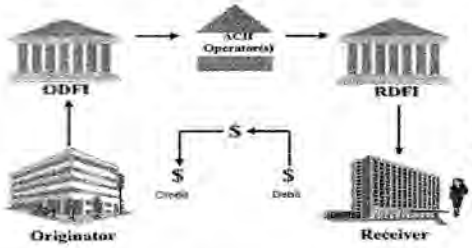
The audit function should be staffed appropriately with auditors who have sufficient expertise to evaluate all aspects of the ACH program. The board should ensure that there is sufficient expertise to carry out the bank's ACH audit activities, whether the function is performed by internal audit staff or an external audit firm. The board should also ensure that auditors attend training periodically to ensure that their skills keep pace with any expansion in the bank's ACH program.

Credit Risk

Banks' credit-risk exposures have increased significantly with the expansion into higher-risk ACH activities such as nonrecurring payments. Credit risk occurs in different forms, depending on the type of transaction and the bank's role in the transaction. For ACH *credit* entries, the originating bank (ODFI) incurs credit risk upon initiating the entries until its customer funds the account at settlement. The receiving bank (RDFI) incurs credit risk if it grants its customer funds availability prior to settlement of the credit entry. For ACH *debit* entries, the ODFI incurs credit risk from the time it grants its customer funds availability until the ACH debit can no longer be returned by the RDFI. [5] The RDFI's credit risk from a debit entry rises if it allows the debit to post and overdraw its customer's account. *(See Figure 1.)*

Banks need to implement credit-risk controls that establish underwriting standards, require analysis of originators' creditworthiness, and set appropriate credit exposure limits. Banks with more complex ACH programs or banks that do not mitigate credit risk through holdbacks or reserve accounts will need to develop more expansive credit-risk management systems.

Figure 1 - Depicts the funds flow for an ACH debit transaction [6]



Establishing Originator Underwriting Standards

As with other types of credit exposures, each bank's loan policies should include formal underwriting standards and an approval policy for ACH originators. During an initial review of originator information, banks typically reject originators that have a history of excessive unauthorized returns, or that do not operate a legitimate business. The depth of a bank's initial review should match the level of risk posed by the originator.

Underwriting standards enable bank management to clearly communicate the process and documentation required for approving new originators and expanding existing originators' ACH activities. Under the board's direction, bank management should implement underwriting standards for all originators. Such standards generally

- Define desirable, prohibited, and restricted originators [7] ;
- Require a background check of the originator to validate the legitimacy of the business (if necessary, this check can be supplemented with a background check on the principal business owners of the originator);
- Require evaluation of the originator's creditworthiness, including a comprehensive financial analysis (similar to that performed on other potential unsecured borrowers);
- Outline the type and timing of financial information to be provided by the originator;
- Require review of the originator's sales history;
- Summarize documentation requirements, including social security number or tax identification number;
- List permissible Standard Entry Class (SEC) types [8] ;
- Provide authorization procedures for approved originators;
- Provide guidelines for setting exposure limits, including requirements for pre-funding or collateral requirements;
- Establish overlimit monitoring and approval;
- Outline originator account termination procedures; and
- Allow the bank to audit originators' ACH processes and controls at the bank's discretion.

Banks should use the underwriting standards listed above as guidance, to be adapted as necessary to reflect each bank's specific circumstances and individual risk profile. Banks engaged in complex or high-risk ACH transactions should implement more stringent underwriting standards than banks that only conduct traditional, lower-risk ACH transactions.

Risk Selection - Analyzing Originator Creditworthiness and Establishing Exposure Limits

Banks should perform ongoing credit analysis on ACH originators. Analyzing creditworthiness is a critical step in establishing and monitoring appropriate exposure thresholds for the type and volume of transactions processed by the bank. Banks should approach ACH credit analysis the same way they

evaluate other credit arrangements by considering the proposed activity (such as purpose of the loan), and determining through financial and other analysis how much unsecured credit to extend. The bank should maintain a credit file on the originator that will include the types of ACH transactions that are authorized, the bank's financial analysis and evaluation of creditworthiness, and approved exposure limits for daily and multi-day settlements.

To manage credit risk effectively, banks should set ACH credit and debit exposure thresholds for originators and monitor the appropriateness of, and compliance with, such limits on a regular basis. Consistent with NACHA requirements, banks should establish separate exposure limits and monitoring practices for WEB entries. Banks should also implement procedures to monitor ACH entries relative to the exposure limit across multiple settlement dates. Banks need to be aware of the extended return time frames for consumer debit transactions. [9] Management should

- Set limits and obtain appropriate internal approvals before allowing ACH transactions to be initiated;
- Establish processes to ensure bank management remains abreast of originators' ongoing financial condition so management can take timely mitigating action, such as amending exposure limits or requiring pre-funding; and
- Implement a process to ensure that approvals of over-limit transactions are well controlled and consistent with the bank's policies for extending unsecured credit.

In cases in which the bank requires pre-funding before transactions are originated through the ACH network, the bank should ensure that it has collected funds before an ACH file is sent to the ACH Operator. Banks require pre-funding for a variety of circumstances, but, at a minimum, should impose such requirements on troubled borrowers. [10]

To further reduce credit risks, management should implement procedures that require lending and ACH operations personnel to consult with one another at least annually or more often, if necessary, to confirm that the originator's financial condition has not changed from the time the credit facility was approved. [11]

High-Risk Activities

Banks that engage in ACH transactions with high-risk originators or that involve third-party senders face increased reputation, credit, transaction, and compliance risks. High-risk originators include companies engaged in potentially illegal activities or that have an unusually high volume of unauthorized returns. High-risk originators often initiate transactions through third-party senders because they have difficulty establishing a relationship directly with a bank.

Examples of high-risk parties include online payment processors, certain credit-repair services, certain mail order and telephone order (MOTO) companies, illegal online gambling operations, businesses located offshore, and adult entertainment businesses. These operations are inherently more risky and incidents of unauthorized returns are more common with these businesses. [12]

Before a bank engages in high-risk ACH activities, the board of directors should consider carefully the risks associated with these activities, particularly the increased reputation, compliance, transaction, and credit risks. The board should provide clear direction to management on whether, or to what extent, the bank may engage in such ACH activities. Some banks have established policies prohibiting transactions with certain high-risk originators and third-party senders.

Banks that engage in high-risk ACH activities should have strong systems to monitor and control risk. These systems should monitor the level of unauthorized returns, identify variances from established parameters such as origination volume, and periodically verify the appropriate use of SEC codes, as transactions are sometimes coded incorrectly to mask fraud. [13] In addition, transactions with higher-risk elements, such as TEL and WEB, should be monitored to ensure that they are within the institution's risk tolerance. A high level of unauthorized returns is often indicative of fraudulent activity. [14] This indication may prompt management to terminate the relationship with the originator or third-party sender, or signal that additional training is needed to ensure compliance with ACH rules.

Compliance Risk

A bank's compliance risk management system should incorporate applicable policies, procedures, and processes for its ACH activities, including those conducted through third parties. [15] ACH reviews should be comprehensive and should test for compliance with a number of regulatory requirements, including Regulations CC, DD, and E, Bank Secrecy Act/Anti-Money Laundering (BSA/AML) and Office of Foreign Assets Control (OFAC) requirements, and NACHA and other network rules.

If the bank's compliance review detects regulatory violations or errors on a consumer's account, bank management should correct them in a timely manner. Remedial action includes the timely crediting of the consumer's account, identifying the cause of the violation or error, and implementing any new policies, procedures, or controls needed to prevent recurrence.

The Bank Secrecy Act requires banks to have BSA/AML compliance programs and appropriate policies, procedures, and processes in place to monitor and identify unusual activity, including ACH transactions. [16] ACH transactions that are originated through a third-party service provider (when the originator is not a direct customer of the ODFI) may increase BSA/AML risk. Risks are heightened when neither the third party nor the ODFI performs due diligence on the companies for which they are originating payments. [17]

For relationships with a bank's or an originator's third-party service provider, CDD on the third-party service provider can be supplemented with due diligence on the principals associated with the third-party service provider. When a bank is heavily reliant upon its third-party service provider, it should review the third-party service provider's suspicious-activity monitoring and reporting program, either through its own or an independent inspection. [18]

ACH transactions can be used in the layering and integration stages of money laundering. Detecting unusual activity in the layering and integration stages can be a difficult task, because ACH may be used to legitimize frequent and recurring transactions. Banks should consider the layering and integration stages of money laundering when evaluating or assessing the ACH transaction risks of a particular customer. Because of the nature of ACH transactions, adequate and effective customer and originator due diligence policies, procedures, and processes are critical in detecting unusual and suspicious activities.

Equally important is an effective risk-based suspicious activity monitoring and reporting system. For banks originating transactions for noncustomers (i.e., through third parties), the suspicious-activity monitoring and reporting systems should include the monitoring of ACH detail activity when the batch-processed transactions are returned or separated for other purposes. [19]

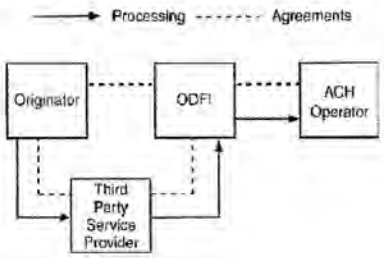
The ODFI may need to more closely scrutinize transaction details for international ACH activities. [20] The ODFI, if frequently involved in international ACH, may develop a separate process for reviewing international ACH transactions that minimizes disruption to general ACH processing, reconcilement, and settlement.

All parties to an ACH transaction are subject to the requirements of OFAC. With respect to domestic ACH transactions, the ODFI is responsible for verifying whether the originator is not a blocked party and for making a good faith effort to determine that the originator is not transmitting blocked funds. The RDFI similarly is responsible for verifying that the receiver is not a blocked party. ODFIs are not responsible for unbatching transactions if they receive those transactions already batched from their customers who have been placed on notice about their own responsibilities with regard to OFAC regulations. In such cases, ODFIs may rely on RDFIs for compliance with OFAC requirements with respect to blocking accounts and transactions on the RDFI's books. However, to the extent that unbatching occurs, the ODFI is responsible for screening as though it had done the initial batching. With respect to OFAC screening, these same obligations hold for cross-border ACH transactions. For outbound cross-border ACH transactions; however, the ODFI cannot rely on OFAC screening by the RDFI outside of the United States.

Third-Party Service Providers

The use of third parties in ACH transactions adds complexity and increases a bank's exposure to compliance, credit, transaction, and reputation risks. Use of third-party service providers, which conduct activities on behalf of a bank, increases risk because the bank remains legally responsible, but does not have direct control over the functions performed by the third party. *(See Figure 2.)* Risks are even higher when the third party is permitted direct access to the ACH Operator on behalf of the bank. [21] Bank management should effectively oversee all ACH activity that is conducted through the bank. [22]

Figure 2 - Depicts the funds flow of a Third-Party Service Provider [23]

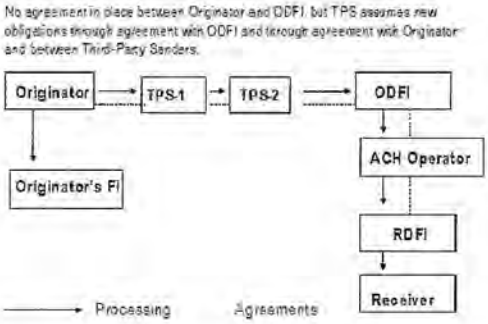


To effectively manage risk from third-party service providers, bank management should establish procedures that allow the bank to monitor the third-party service provider's operations. The first step in this process is identifying and validating the third party and the type of business it conducts. Banks should check thoroughly the background of each third-party service provider, including the principal owners, and also verify the organization's financial capacity to absorb losses. This step is particularly important if the bank allows the third party to have direct access to the ACH Operator.

Third-Party Senders

Third-party senders are bank customers to which originators outsource payment services, but the bank has no direct customer or contractual relationship with the originator. The third-party sender provides services to the originator and, in that capacity, acts as an intermediary between the originator and the ODFI. Because of the complexity of these arrangements, banks often lack appropriate controls over activities involving third-party senders. *(See Figure 3.)*

Figure 3 - Depicts a Third-Party Sender (TPS) acting as an intermediary between an Originator and ODFI [24]



Banks that initiate ACH transactions for third-party senders should know, at a minimum, for which originators they are initiating entries into the ACH network. Thus, banks should require third-party senders to provide certain information on their originator customers such as the originator's name, taxpayer identification number, principal business activity, and geographic location. Also, before originating transactions, a bank should verify (directly or through a third-party sender) that the originator is operating a legitimate business. [25]

Banks should be alert to whether third-party senders are using more than one bank to originate transactions. Third parties that use multiple banks to originate ACH transactions require greater scrutiny before being approved to originate transactions through the bank. For example, some third-party senders may use multiple banks to process their transactions because they had their contract with another bank terminated.

To effectively manage the risk from these arrangements, banks should have strong oversight of all third-party senders. Bank management should stay abreast of the ongoing financial condition of third-party senders and take timely mitigating action, such as amending exposure limits or requiring pre-funding. Bank management should establish a written agreement with each third-party sender. Generally, these agreements

- Outline the specific board-approved risk parameters within which the third-party sender must operate;
- Detail the obligations and liabilities of the third-party sender;
- Define the information that must be provided to the bank before the third-party sender can submit transactions for a new originator;
- Define approved and disallowed originator and transaction types;
- Provide the bank ongoing access to all originators' files; and
- Outline the bank's right to audit periodically such files and/or third parties so that the bank can verify the third-party sender's compliance with bank policies.

Bank management should also ensure that there is a process to monitor third-party senders, and should establish a system to audit periodically such senders to ensure that they are operating in a sound manner.

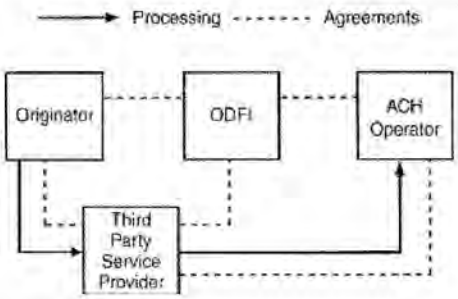
Direct Access to the ACH Operator

A bank that permits an originator or a third party (either its third-party service provider or an originator's third-party sender) to have direct access to the ACH Operator should maintain control over its own settlement accounts at all times. *(See Figure 4.)* To do so, a bank should enter into a written contract

with the party granted access outlining the rights and responsibilities of the parties, and include a provision permitting the bank to audit the party granted access, as needed, to monitor performance and ensure compliance with applicable laws and regulations. Written contracts usually include:

- A requirement that the party granted access obtain the bank's prior approval before originating ACH transactions under the bank's routing number.
- Bank-established dollar limits for files that the party granted access deposits with the ACH Operator. A file that exceeds these dollar limits should be brought to the bank's attention before being deposited with the ACH Operator so the bank can either approve it as an exception or require that it be held until the next business day.
- A provision that restricts the other party's ability to initiate corrections to files. The bank should implement with the ACH Operator risk-control measures that limit the correction ability of the party granted access. If bank management allows the other party to correct files, it should impose and enforce strict controls over these corrections. Specifically, management should first authorize any changes to the file totals and then instruct the ACH Operator to release the file for processing. This should be a positive check-off process; *i.e.*, the ACH Operator should receive the authorization to process a file, and failure to receive the authorization should result in the file being deleted. In this way, the bank has control over its exposure from files processed by the other party.

Figure 4 - Depicts a Third-Party Service Provider with direct access to the ACH Operator [26]



Transaction Risk

Many banks process payments across different retail and wholesale payment systems for example ACH, credit card, debit card, check, and wire that add complexity to transaction-risk management. An effective ACH risk management program should be designed to coordinate with other retail and wholesale payment-risk management programs to mitigate total bank risk exposure. An effective ACH risk management program may not reduce a bank's total risk exposure if activities are allowed to migrate to other payment systems. The industry has identified this additional complexity as "cross-channel risk."

Information Technology

Banks frequently deliver ACH services through a complex technology environment. Bank ACH systems use multiple applications, processing, storage, and communications systems that can be accessed by many internal and external users. Those systems may be operated by the bank, bank customers, or various service providers. An ACH Operator will be used for transaction clearing and settlement. Moreover, many of the communications and processing systems necessary to provide ACH services are not unique to those services. Effective risk management of the complex ACH technology environment

requires a disciplined approach to the identification, measurement, and management of technology-related risks.

The *FFIEC Information Technology Examination Handbook*, through a series of 12 booklets, provides guidance in appropriately assessing the various risks associated with technology, employing effective strategies and controls, and monitoring and testing the provision of services to provide assurance that the risks are appropriately mitigated. Many of the booklets are relevant to the systems used to provide ACH services, and the "Retail Payments Systems Booklet" provides additional specific guidance related to ACH systems. [27]

Banks should maintain consistent and effective controls over the technology used to provide ACH services, especially in the key control functions of information security and business continuity.

Information Security

ACH-related systems, processes, and controls should be included in a bank's information security program. Additionally, banks should ensure that their online ACH services comply with OCC Bulletin 2005-35, Authentication in an Internet Banking Environment. [28] (See also, OCC Bulletin 2006-35, (frequently asked questions). [29] At a minimum, the bank's information security program should address

- Customer access - Bank management should ensure dual control and confidentiality in the initial setup and activation of new customers regardless of the communication channel. Similarly, banks should secure the distribution and reset process for any authenticators used to access ACH services.
- Employee access - Banks should minimize and monitor the number of personnel with access to systems that support ACH services. Banks should minimize and segregate ACH staff and limit access to various maintenance and transaction support functions (i.e., changing account numbers, adding or deleting new users, changing transaction limits.).
- Data security - Banks should ensure that sound, risk-based data security controls exist across all ACH-related systems, applications, and processes. Control policies and practices should address data in transit or storage. ACH operations staff should accept data only from properly authenticated sources and provide a secure communication channel for all critical or confidential data. Banks should identify confidential or critical data used in ACH operations and ensure that proper storage and disposal practices are used. Key practices might include purging data from online applications, encrypting data, and destroying trace data from any media.

Business Continuity Planning

A bank's ACH activities should be factored into the bank's overall business continuity plans. Business units should ensure up-to-date assessments in light of the increased corporate-wide and customer reliance on the availability of ACH services. The business unit plans should carefully map interdependencies between units that support ACH services. Banks should also ensure that business continuity test plans are consistent with the criticality and complexity of the supporting operations for ACH services. Some business units may need to increase the scope of their testing to ensure coordinated testing with other units or key infrastructure components, such as mainframe operations, network services, or telecommunications.

Conclusion

The OCC supports national banks' participation in the ACH network to serve the needs of legitimate bank customers and to diversify sources of revenue. To maximize the benefits of ACH activities, banks should implement an effective process for managing the associated risks. The value a bank will derive from its ACH program is directly proportional to the quality of the board's strategic planning and the effectiveness of its ACH risk management program.

Additional Information

You may direct any questions or comments to the Operational Risk Policy Division at (202) 649-6550.

Mark L. O'Dell
Deputy Comptroller for Operational Risk

[1] http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html (http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html).

[2] See NACHA Operating Rules on the Internet at http://www.nacha.org/c/ach.rules.cfm

[3] ACHA operating rules provide that originators must allow consumers to opt out of ARC check conversion and establish reasonable procedures under which consumers may notify originators that their checks are not to be converted.

[4] At a minimum, returns rates should be reviewed at the originator level for all originators.

[5] ODFIs generally charge back a returned ACH debit to the originator. But the ODFI may suffer a loss if, for example, the originator's account has insufficient funds or has been closed.

[6] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.

[7] Originators are generally classified based on their principal business activity, and in some cases their geographic location (e.g., some banks may choose to not act as the ODFI for originators located outside of the United States). For additional information on restricted merchants and risk management related to merchant underwriting, refer to the Merchant Processing booklet of the Comptroller's Handbook (2001).

[8] The SEC Code identifies the specific computer record format that will be used to carry the payment and payment-related information.

[9] Consumer debit transactions may be returned for certain reasons (such as a consumer believes that the transaction is not authorized) through the ACH network for up to 60 days. In addition, an ODFI's potential liability under the NACHA Rules for breach of warranty is not limited to the return time frames, but is limited only by the statute of limitations for breach of contract claims under applicable law. See NACHA Operations Bulletin (Mar. 28, 2003).

[10] A troubled borrower is defined as having credit rated by the OCC as special mention, substandard, doubtful, or loss, or adversely rated by the bank's internal rating system.

[11] Some banks may choose to use the same risk management policies and procedures they use for short-term unsecured extensions of credit to manage the risk associated with merchants and commercial customers originating ACH transactions.

[12] Risks may include the risk of legal liability or damage to an institution's reputation when originators or third-party senders facilitate or engage in activities that violate criminal laws.

[13] Fraud analysts should not rely exclusively on excessive unauthorized returns to identify fraud. Unusually high levels of returns for other reasons (e.g., nonsufficient funds (NSF), invalid account, or account not found) may also be indicative of fraud for some originators.

[14] NACHA operating guidelines state that a return rate of 2.5 percent is well above the acceptable rate for normal business purposes.

[15] The terms "third-party service provider" used in the Compliance section of this guidance means a third-party service provider or a third-party sender, or both, depending on the context.

[16] The FFIEC's Bank Secrecy Act/ Anti-Money Laundering Examination Manual provides additional information on BSA/AML, OFAC, and CDD requirements for ACH transactions.

[17] Ibid [http://www.ffiec.gov/bsa_aml_infobase/default.htm], page 196.

[18] Payment processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, and fraud schemes. For additional information, refer to the Third-Party Payment Processors section of the FFIEC's BSA/AML Examination Manual.

[19] Additional information on suspicious activity monitoring and reporting systems can be found in the Automated Clearing House Transactions - Examination Procedures section of the FFIEC's BSA/AML Examination Manual.

[20] The ODFI should also apply increased due diligence for domestic ACH transactions when the originator is based in a foreign country.

[21] A third-party service provider may transmit ACH transactions directly to an ACH Operator using the bank's routing number, provided it has obtained permission from the bank. However, the bank warrants the validity of each entry transmitted by the service provider, including the basic requirement that a receiver has authorized each entry.

[22] For additional guidance on managing third-party relationships, refer to OCC Bulletin 2001-47.

[23] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.

[24] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.

[25] Bank management should ensure that the bank's audit program checks for adherence to bank policy in third-party sender arrangements.

[26] Copyright held by NACHA. Reprinted with the permission of NACHA. All rights reserved.

[27] FFIEC Retail Payments Handbook. http://www.ffiec.gov/ ffiecinfobase/html_pages/retail_book_frame.htm

[28] OCC Bulletin 2005-35

[29] OCC bulletin 2006-35

* References in this guidance to national banks or banks generally should be read to include federal savings associations (FSA). If statutes, regulations, or other OCC guidance is referenced herein, please consult those sources to determine applicability to FSAs. If you have questions about how to apply this guidance, please contact your OCC supervisory office.

Office of the Comptroller of the Currency
U.S. Department of the Treasury

OCC BULLETIN 2008-12

Subject: Payment Processors
Date: April 24, 2008

To: Chief Executive Officers, Chief Risk Officers and Compliance Officers of All National Banks, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

Description: Risk Management Guidance

As of October 30, 2013, this guidance applies to federal savings associations in addition to national banks.*

Purpose

This bulletin presents guidance to national banks for due diligence, underwriting, and monitoring of entities that process payments for telemarketers and other merchant clients. As detailed in several OCC issuances, certain merchants, such as telemarketers, pose a higher risk than other merchants and require additional due diligence and close monitoring. This bulletin supplements, but does not replace, existing guidance related to Automated Clearing House (ACH) risk management, merchant processing, and remotely-created checks (RCCs).

Background

The OCC has seen a variety of relationships between banks and processors in which the processor uses its bank relationship to process payments for merchant clients. Often the processor uses a bank account as the vehicle to conduct such payment processing. For example, a processor may be a bank customer that deposits into its account RCCs generated on behalf of merchant clients. A processor may also act as a third-party sender of ACH transactions, originating debits for its merchant clients through its customer relationship with the bank. In either case, the bank often has no direct customer relationship with the merchant. Risks are heightened when neither the processor nor the bank performs adequate due diligence on the merchants for which they are originating payments.

When a bank has a relationship with a processor, it is exposed to risks that may not be present in relationships with other commercial customers. The bank encounters strategic, credit, compliance, transaction, and reputation risks in these relationships. Banks have two distinct areas of responsibility to control these risks. The first is due diligence and underwriting, and the second is monitoring these high-risk accounts for high levels of unauthorized returns and for suspicious or unusual patterns of activity. Proper initial due diligence, effective underwriting, and ongoing account monitoring are critical for bank safety and soundness and consumer protection. Banks should implement these controls to reduce the likelihood of establishing or maintaining an inappropriate relationship with a processor through which unscrupulous merchants can gain access to consumers' bank accounts.

Banks should also consider carefully the legal, reputation, and other risks presented by relationships with processors including risks associated with customer complaints, returned items, and potential unfair or deceptive practices.† Banks that do not have the appropriate controls to address the risks in these relationships may be viewed as facilitating a processor's or its merchant client's fraud or other unlawful activity. Banks should be alert for processors that use more than one bank to process payments for merchant clients and should subject such processors to great scrutiny. Processing through multiple banks may be a signal that the processor recognizes a risk that one or more of these processing relationships

may be terminated as a result of suspicious, fraudulent, or other unlawful conduct.[2]

Risk Management: Effective Due Diligence, Underwriting, and Monitoring

The OCC has provided guidance to national banks regarding relationships with processors. For example, banks must implement a due diligence and underwriting policy that, among other things, requires an initial background check of the processor and its underlying merchants to support the validity of the processor's and merchants' businesses, their creditworthiness, and business practices.[3] Moreover, the OCC has also provided banks detailed procedures for merchant underwriting and review, as well as for fraud monitoring.[4] Banks should review carefully the validity and creditworthiness of all processors and merchants. Controls should be more rigorous for higher-risk processors and merchants (*e.g.*, telemarketers). Although some processors may process transactions for reputable telemarketing merchants, these merchants in aggregate have displayed a much higher incidence of unauthorized returns or chargebacks, which is often indicative of fraudulent activity.

Due diligence, underwriting and account monitoring are especially important for banks in which processors deposit RCCs and through which processors initiate ACH transactions for their merchant clients. Banks should be alert to processors' merchant clients that obtain personal bank account information inappropriately. The merchant may have misused the customer information to facilitate the creation of an unauthorized RCC or ACH debit file by the processor.[5] To ensure effective risk management, banks that initiate transactions for processors should require the processor to provide information on their merchant clients such as the merchant's name, principal business activity, and geographic location.[6] Banks should verify directly, or through the processor, that the originator of the payment (*i.e.* the merchant) is operating a legitimate business. Such verification could include comparing the identifying information against public record databases and fraud and bad check databases, comparing the identifying information with information from a trusted third party, such as a credit report from a consumer reporting agency, or checking references from other financial institutions. With respect to account monitoring, a bank should not accept high levels of returns[7] on the basis that the processor has provided collateral or other security to the bank.

By implementing the appropriate controls over processors and their merchant clients, a bank should be able to identify those processors that process for fraudulent telemarketers or other unscrupulous merchants and to ensure that the bank is not facilitating these transactions. In the event a bank identifies fraudulent or other improper activity with a processor or a specific merchant client of the processor, the bank should take immediate steps to address the problem, including filing a Suspicious Activity Report when appropriate, terminating the bank's relationship with the processor, or requiring the processor to cease processing for that specific merchant.

Banks are required to have Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance programs and appropriate policies, procedures, and processes to monitor and identify unusual activity. Additionally, the FFIEC BSA/AML Examination Manual reiterates the OCC's expectation that banks effectively assess and manage their risks with respect to third-party processors. Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions or transactions prohibited by the Office of Foreign Assets Control. The bank's risk management program should include procedures for monitoring processor information such as merchant data, transaction volume, and charge-back history.[8]

Conclusion

The OCC supports national banks' participation in payment systems to serve the needs of legitimate processors and the customers of such processors and to diversify sources of revenue. However, to limit potential risk to banks and consumers, banks should ensure implementation of risk management programs that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, bank programs should verify the legitimacy of the processor's business operations, assess the bank's risk level, and monitor processor relationships for activity indicative of fraud.

Additional Information

For additional information related to managing the risks associated with retail payment activities please refer to:

- OCC Bulletin 2006-39, ACH Activities: Risk Management Guidance.
- The "Merchant Processing" booklet of the *Comptroller's Handbook*.
- OCC Bulletin 2006-13, Amendments to Regulation CC and J.
- OCC Bulletin 2001-47, Third-Party Relationships: Risk Management Principles.
- The "Outsourcing Technology Services" booklet of the *Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook*.
- The "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook*.
- The *FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

Please direct any questions or comments to the Operational Risk Policy Division at (202) 649-6550.

Mark L. O'Dell
Deputy Comptroller for Operational Risk

---

[1] *See* 15 USC 45. See also OCC Advisory Letter 2002-3, Guidance on Unfair or Deceptive Acts or Practices.

[2] *See, e.g.*, OCC Bulletin 2006-39, p.10.

[3] *See* the "Merchant Processing" booklet of the *Comptroller's Handbook*, pp. 24-28, 34; The FFIEC's Bank Secrecy Act/Anti-Money Laundering Examination Manual, Third Party Payment Processors, and OCC Bulletin 2006-39, pp. 5, 10-11.

[4] *See* the "Merchant Processing" booklet of the *Comptroller's Handbook*, pp. 24-28

[5] Though the Merchant Processing booklet of the Comptroller's Handbook addresses directly merchant card acquiring, its principles and most of the procedures outlined in the handbook are also applicable to the processing of other payment instruments, including RCCs and ACH transactions. *See, e.g.*, OCC Bulletin 2006-39, footnote 7 and associated text.

[6] *See* OCC Bulletin 2006-39. A background check on the principal business owners supplaments the underwriting of the merchant client. It is not uncommon for unscrupulous owners to use multiple business entities to avoid detection.

[7] Generally, a bank should not accept high levels of returns regardless of the return reason. High levels of RCCs or ACH debits returned for insufficient funds can be an indication of fraud.

[8] FFIEC BSA/AML Examination Manual, p. 210 (Third-Party Payment Processors). *See also* OCC Bulletin 2006-39.

* References in this guidance to national banks or banks generally should be read to include federal savings associations (FSA). If statutes, regulations, or other OCC guidance is referenced herein, please consult those sources to determine applicability to FSAs. If you have questions about how to apply this guidance, please contact your OCC supervisory office.

Financial Institution Letters

Third-Party Risk
Guidance for Managing Third-Party Risk

FIL-44-2008
June 6, 2008

Summary: The attached FDIC guidance describes potential risks arising from third-party relationships and outlines risk management principles that may be tailored to suit the complexity and risk potential of a financial institution's significant third-party relationships.

Highlights:
Financial institutions often rely upon third parties to perform a wide variety of services and other activities. An institution's board of directors and senior management are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.

Management should tailor the principles contained in this guidance to each significant third-party arrangement, taking into consideration such factors as the complexity, magnitude, and nature of the arrangement and associated risks. This guidance outlines the potential risks that may arise from the use of third parties and addresses the following four basic elements of an effective third-party risk management program:

- Risk assessment
- Due diligence in selecting a third party
- Contract structuring and review
- Oversight

This guidance is based on and supplements the principles contained in policy guidance that has previously addressed third-party risk in the context of specific functions, such as information technology. This guidance is intended to assist in the effective management of third-party relationships, and should not be considered as a set of required procedures.

Distribution:
FDIC-Supervised Banks (Commercial and Savings)

Suggested Routing:
Chief Executive Officer
Chief Financial Officer
Chief Compliance Officer
Chief Risk Officer

Related Topics:
Risk Management
Third-Party Contracts
Outsourcing Arrangements
FFIEC IT Handbook on Outsourcing Technology Services (June 2004)
Required Notification for Compliance with the Bank Service Company Act

Attachment:
Guidance for Managing Third-Party Risk
Guidance for Managing Third-Party Risk (PDF Help)

Contact:
Senior Examination Specialist Kenyon T. Kilber (Risk Management) at kkilber@fdic.gov or (202) 898-8935, or Policy Analyst Victoria Pawelski (Compliance) at vpawelski@fdic.gov or (202) 898-3571

Printable Format:
FIL-44-2008 (PDF Help)

Note:
FDIC financial institution letters (FILs) may be accessed from the FDIC's Web site at http://www.fdic.gov/news/news/financial/2008/index.html.

To receive FILs electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html.

Paper copies of FDIC financial institution letters may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (1-877-275-3342 or 703-562-2200).

Last Updated 6/6/2008 communications@fdic.gov

Home | Contact Us | Search | Help | Site Map | Forms | En Español
Website Policies | Privacy Policy | Accessibility Statement | Plain Writing Act of 2010 | USA.gov | FDIC Office of Inspector General
Freedom of Information Act (FOIA) Service Center | FDIC Open Government Webpage | No FEAR Act Data

Mr. BACHUS. And at this time the Ranking Member is recognized for 5 minutes.

Mr. JOHNSON. If I might, Mr. Chairman, I would like to—since I am the only—since I am the only Democrat here, I would like to wait until the other Republicans have asked their questions before I ask my questions.

Mr. BACHUS. Mr. Marino, would you like to be recognized?

Mr. MARINO. Thank you. Thank you, Chairman.

Thank you, Ranking Member.

Assistant Attorney General, welcome. I am sure you did a little reading on us beforehand and know that my background and my colleague to the right, Mr. Holding—we were U.S. attorneys and district attorney. I was a district attorney as well.

And there is no one here in D.C. that is more of a law enforcement guy than I am. I have the utmost respect for U.S. attorneys and prosecutors. I have—had a great deal of pride and still do to work at Justice and to be nominated.

I do have a concern with what is taking place—what appears to be taking place.

You have been the one to be chosen to be here and explain. I give you courage for stepping up to the plate and doing that. It should reflect in your review when that comes up, and I think you are warranted a raise.

But, given that, "fraud" is a very vague term. And we, as prosecutors, you, as a prosecutor—we have a great deal of power. You probably have more power than anybody on Earth when it comes to investigations, whether it is civil or criminal, and we know that civil cases do turn into criminal cases.

And I had the same philosophy as you do. Follow the money. I did it with drug dealers. I did it with organized crime. I did it with money laundering.

My concern is—I want you to, if you would, please, convince me that this is not a witch hunt, that this is not the Department of Justice—let's forget about the White House and the Administration.

Because I always felt the Department of Justice—although I worked for the President, we were and are an independent agency that enforces the rule of law, not politics.

And if memory serves me right—and I looked things up and memory does serve me right—that there is no definition in "fraud."

We talk about wire fraud or security fraud. There is really no definition in the Federal statute. Courts have made the determination as what the definition is.

And just—I taught constitutional law a little bit, and I want to refer back to jury instructions that courts—that I have had courts use on describing to a jury what fraud is.

And there is a lot more to this. But it is a general term which embraces an ingenious effort, all ingenious efforts, and means that individuals devise to take advantage of others. We, as prosecutors, can interpret that in numerous ways.

Please tell me that that is not being used for political reasons.

Mr. DELERY. Well, Congressman, I can certainly tell you that it is not in the matters that I supervise and more broadly.

And I am happy to address the issues that you have raised because I do agree with your general approach and I think that it is important for us to respond.

And so I guess what I would do is point to the origin of these cases and how we came to pursue them and, as the best evidence of what these cases are about, the one that I mentioned earlier, Four Oaks, which was actually done in partnership with Mr. Holding's former district in North Carolina.

And, you know, our policy in these cases is to investigate specific evidence of fraud based on evidence that consumers are being harmed, are being defrauded, not whole industries or businesses acting lawfully.

We are holding financial institutions accountable for their own misconduct, for their own fraudulent conduct, not for the misconduct of anybody else.

And so, if you look at Four Oaks, Four Oaks was a bank that facilitated transactions by a payment processor, even though it had hundreds of sworn complaints about unauthorized transactions, it had received warnings from NACHA, which is the electronic payments association, it received a warning by the Arkansas Attorney General's Office——

Mr. MARINO. I am familiar with that, and I have followed the facts on it.

But you did make a statement that—you said, "We at Justice decided to pursue these fraud cases."

Was it you that decided to pursue? Was it someone above you? Was it the attorney general or the DAG? Or did it come from the White House?

Mr. DELERY. So it came—it originated as a proposal from career lawyers in the Justice Department who had spent many years working on cases involving fraudulent merchants. And, based on that work, following the money, they noted the involvement of—knowing involvement of some payment processors and banks. And that was the genesis of these cases. And it was under my authority in the Civil Division that it was done.

Mr. MARINO. I think I am well over my time. We have to go and vote.

But just as a prosecutor, promise me this, that we are following the law, that you are following the law, that these are genuine fraud cases that are not manipulated to look like fraud cases, and that we, as prosecutors, have a responsibility to focus on the rule of law and nothing else.

Mr. DELERY. I agree, Congressman. That has been the policy of these cases from the beginning and will continue to be.

Mr. MARINO. Thank you. I yield back.

Mr. BACHUS. Thank you.

We have votes on the floor. So we will be recess—how many votes are there? Three votes. So we will——

Mr. Smith, you could go ahead, but I think it is—there is only 3 minutes left on the floor.

Would you prefer to ask a question or two?

Mr. SMITH. Could I ask quickly?

Mr. BACHUS. Okay. Go ahead. I am going to recognize Mr. Smith.

Mr. SMITH. Thank you, Mr. Chairman.

My question—I have two. Has anyone at DoJ voiced concerns that Operation Choke Point could go too far and harm entire industries?

Mr. DELERY. Well, certainly, we have heard some of the reports that—you know, there have been reports in the press. We have had letters from Members of Congress. And we always take seriously the question about whether our efforts to combat fraud are affecting institutions that we are not, in fact, investigating.

So that is something that we always are mindful of and take into account and review what we are doing to avoid those—those effects, and we are doing that in connection with these cases.

Mr. SMITH. So has anyone voiced concern at DoJ?

Mr. DELERY. I think what I would say is that we have responded—we have—we have heard the concerns that people have been expressed—that people have expressed and have responded by not only looking at what we are doing, but, also, taking affirmative steps to make clear to the public and to industry what our policy is about these cases, what we are and are not doing, so that we can avoid any unintended effects that go beyond what we are trying to do, which is to hold institutions accountable for fraud that they are committing.

Mr. SMITH. How many institutions have you all prosecuted from Operation Choke Point?

Mr. DELERY. So this set of cases grew out of some prior work, including the Wachovia case that was mentioned earlier. But of the ones—of the investigations that began, you know, in late 2012, early 2013, we have one resolution, the Four Oaks Bank case. There are other investigations that are still in process.

Mr. SMITH. So only one from Operation Choke Point?

Mr. DELERY. As I indicated, there are other investigations still in process, but only one res—one of them has been resolved at this point.

Mr. SMITH. Okay. You were in private practice at a private law firm. What is your estimate of the costs to comply with the average subpoenas that DOJ sent out under Operation Choke Point?

Mr. DELERY. Congressman, I don't know what the estimate would be. I think that, in this context, we have sent subpoenas where we had reason to believe that the recipient either—the recipient had information about fraudulent conduct, either its own or on behalf of somebody else.

Because sometimes subpoenas seek information, you know, related to third parties. And, as is usually the case, we have a dialogue with the recipients to discuss the scope and how the best attempts—what the best process would be for responding.

Mr. SMITH. I think it is very important that any government agency, any Federal agency, let alone DOJ—that if they are asking or requesting something out of any industry or any individual or any taxpayer, they better know the ramifications of their ask and how much it is going to cost them. And the fact that you don't have any idea is very disheartening to me.

Mr. DELERY. And I think that that is something that our lawyers keep in mind as they are framing the—framing the subpoenas, to target them to the information that we need, and that is something

that we are—we are mindful of in this and all of the other areas that we pursue.

Mr. SMITH. You need to be more diligent to make sure you can understand how much of a financial impact your asks are going to have on private industry and private citizens before you start asking.

Thank you, Mr. Chairman.

Mr. BACHUS. Thank you.

And at this time we will recess for votes on the floor and then we will return at the termination of those votes. Thank you.

Mr. DELERY. Thank you, Mr. Chairman.

Mr. ISSA [presiding]. The Committee will come back to order.

The gentleman from Georgia is recognized.

Mr. JOHNSON. Thank you, Mr. Chairman.

This hearing appears to be in keeping with a couple of hearings that I have been associated with this week having to do with allegations of Presidential overreach, abuse of authority, even murmurs of impeachment. And this is a hearing that is in keeping with the spirit of those hearings.

One hearing yesterday, in Armed Services, the Committee approved a subpoena for emails from Lois Lerner of the IRS. And then the Justice Department had a similar hearing. And so we are Benghazi, we are IRS, and now we are into the subject of the big Wall Street banking industry being singled out by this Administration, and being singled out for persecution and criminal prosecution because of allegations, unfounded allegations of consumer fraud and other alleged offenses.

So far, I mean, a hearing, "Guilty Until Proven Innocent? A Study of the Propriety and Legal Authority for the Justice Department's Operation Choke Point." Well, I have not heard any questions about the improper use of authority, legal authority, for the Justice Department's Operation Choke Point. And I have heard nothing about any financial service corporation being singled out for prosecution in the Justice Department's Operation Choke Point.

Mr. ISSA. Would the gentleman yield?

Mr. JOHNSON. Yes.

Mr. ISSA. My staff has informed us that, from the 50 subpoenas that were issued, only one was to a large bank and it wasn't a Wall Street bank. The 50 subpoenas that we know of were issued to credit unions and small community banks. I just wanted make sure the gentleman from Georgia knew that.

Mr. JOHNSON. And that is a point well taken. But I think this hearing has devolved into a semi-spectacle with allegations of industry profiling, and I think we have kind of blown up some legitimate investigations and one civil action by the Justice Department into a misuse of authority by the President, oppressing banks. And this is not the case. And I am glad that my friend on the other side recognizes that.

But I do want to ask you, sir, about the complaint filed against Four Oaks Bank. The Justice Department's complaint against Four Oaks Bank is the only civil action against any party as a result of Operation Choke Point. Isn't that correct?

Mr. DELERY. Yes, Congressman, it is one that has been filed.

Mr. JOHNSON. And this is a community bank, or a regional bank, or a large commercial bank.

Mr. DELERY. Well, Four Oaks, I would say, I am not sure how to define it, it is probably regional, is how you would explain it. But I think one of the things that the evidence that we found, as reflected in the complaint, demonstrates is that an institution like that can process a very large number of transactions, more than 9 million for a single payment processor at $2.4 billion. So the numbers that we are talking about can be very large.

Mr. JOHNSON. And in the complaint filed against Four Oaks Bank under FIRREA by the Department of Justice, the United States of America alleged that the bank "knew or was deliberately ignorant of the use of its accounts and its access to the national banking system in furtherance of a scheme to defraud consumers," end quote. Although this complaint was settled, how would a court construe this actual fraud under FIRREA?

Mr. DELERY. I think if you look at the detailed allegations in the complaint, there was clear evidence of widespread information that the bank had about fraudulent transactions that it was processing. That information came from a number of categories, including complaints, sworn complaints by customers who had been victimized, by warnings from a State attorney general and from another organization, had evidence that one of the merchants was attempting to hide its identity, and it had very high return rates for more than a dozen merchants that were more than 30 percent—one was more than 70 percent—which, again, is a strong indication of fraud. Bank officials knew this information and, according to the complaint, continued to process it anyway. And that was the basis for the FIRREA action in that case.

Mr. BACHUS [presiding]. Thank you.

Mr. JOHNSON. Well, now you didn't sue Four Oaks Bank because it provided services to high risk merchants, did you?

Mr. DELERY. The basis for the action was that the bank knew, knowingly facilitated, and in certain circumstances turned a blind eye to evidence that it had of fraud. So I do think that this case is a good example of the work that we are doing, which is to hold banks accountable for their own unlawful conduct under existing law.

Mr. BACHUS. Thank you.

Mr. JOHNSON. Well, as a taxpayer I want to thank you for doing that.

And I will yield back.

Mr. BACHUS. Thank you, Mr. Johnson.

At this time, I recognize Mr. Issa.

Mr. ISSA. Thank you, Mr. Chairman.

Thank you for being here today. I have got a number of questions.

First of all, I would ask unanimous consent that the subpoena dated May 20, 2013, from the Department of Justice Consumer Protection Branch be placed in the record at this time.

Mr. BACHUS. Without objection.

[The information referred to follows:]

U.S. Department of Justice
Consumer Protection Branch

Joel Sweet
Phone: 202-532-4663
Fax: 202-514-8742

Overnight Delivery Address
450 Fifth Street, NW, Sixth Floor South
Washington, D.C. 20001

Mailing Address
P.O. Box 386
Washington, D.C. 20044

[redacted]

VIA CERTIFIED MAIL

[redacted]

RE: Consumer Fraud Investigation

Dear [redacted]

Enclosed is a subpoena requiring the production of documents in connection with an investigation of consumer fraud. We look forward to your cooperation with our investigation.

For your information, also enclosed is regulatory guidance concerning risks posed to banks and consumers by third-party payment processor relationships. See Risk Associated with Third-Party Payment Processors (FIN-2012-A010) (October 22, 2012), Payment Processor Relationships-Revised Guidance (FDIC FIL-3-2012) (January 31, 2012), and Payment Processors-Risk Management Guidance (OCC-2008-12) (April 24, 2008).

If you have any questions, please contact me at 202-532-4633, or Trial Attorney Josh Burke at 202-353-2001.

Very truly yours,

JOEL M. SWEET
Trial Attorney

Enclosures

cc: Josh Burke

U.S. Department of Justice

Civil Division

Office of the Assistant Attorney General *Washington, DC 20530*

SUBPOENA DUCES TECUM
FOR THE PRODUCTION OF DOCUMENTS

TO: [redacted] [redacted]

This subpoena is issued pursuant to 12 U.S.C. § 1833a(g)(1) in the course of an investigation to determine whether there is or has been a violation of one of the provisions of Title 18, United States Code, enumerated in 12 U.S.C. § 1833a(c).

You are hereby required to produce all documentary material described in Exhibit A attached hereto in accordance with the attached definitions and instructions that is in your possession, custody, or control, and to make it available at 450 Fifth Street, NW, 6th Floor South, Washington, DC 20001, for inspection and copying or reproduction. Such production shall occur on or before June 14, 2013. In lieu of production, you may deliver the documentary material to Postal Inspectors Jan Bodon and/or Edward Kljunich, Department of Justice, at the address set forth below.

The production of documentary material in response to this subpoena must be made under a sworn certificate, in the form set forth, by a person or persons having knowledge of the facts and circumstances relating to such production.

Inquiries concerning compliance with this subpoena should be directed to:

Jan Bodon and/or Edward Kljunich
U.S. Postal Inspectors
U.S. Department of Justice
Consumer Protection Branch
450 Fifth Street, NW
6th Floor South
Washington, D.C. 20001
202-514-0514

Date: [redacted]

STUART F. DELERY
Acting Assistant Attorney General
Civil Division

EXHIBIT A

I.
INSTRUCTIONS

A. Documents sought by these requests shall include documents within your knowledge, possession, custody or control, or within the knowledge, possession, custody or control of any of your agents, officers, employees, attorneys or investigators, or any person acting as your representative, including, but not limited to, any otherwise independent accountants or consultants.

B. The fact that some portion of the documents responsive to these requests may already be in the custody of the United States or a United States agency does not excuse compliance with this subpoena.

C. If the Company withholds any document on the ground of any privilege, it shall provide a statement setting forth:

(a) the name and title of the author (and, if different, the preparer and signatory);

(b) the name and title of the person to whom the document was addressed;

(c) the names and titles of all persons to whom the document or a copy of the document was sent or to whom the document or a copy, or any part thereof, was shown;

(d) the date of the document;

(e) the number of pages;

(f) a brief description of the subject matter;

(g) the nature of the privilege claimed; and

(h) the paragraph of the schedule of documents to which it is responsive.

D. No document called for by this subpoena shall be destroyed, modified, redacted, removed, or otherwise made inaccessible, except insofar as documents are withheld under claim of privilege in compliance with the instructions above.

E. If the Company has knowledge of any document that would be responsive to this subpoena schedule but has been lost, destroyed, discarded, or subject to removal or alteration, it shall identify to the extent possible each such document and provide an explanation of the loss, destruction, discarding, removal, or alteration (including identification of each person authorizing or having knowledge of the loss, destruction, discarding, removal, or alteration). Selection of documents from files and other sources shall be performed in such a manner as to ensure that the source and original location of each document may be readily determined.

F. File folders and other containers in which you find documents responsive to these requests, and labels identifying those folders and other containers, shall be produced intact with such documents.

G. The attached "Specifications for Production of ESI and Digitized (Scanned) Images" apply to your production of electronically stored information.

H. Documents must be produced in the same internal order in which they are found in your company's files. Documents that are found stapled, clipped or otherwise fastened together, or in file folders or other enclosures, must be produced in such form and in such folder or enclosure. Documents that are grouped or organized under a single classification or within an individual's selection of files must be produced as a whole without separation, irrespective of the number of distinct paragraphs of this subpoena to which such documents may be responsive. In addition, the name of the person from whose files each such document was produced must be identified.

I. These requests are continuing in nature. You are thus required to amend your responses to these requests and to supplement your production if you learn that your prior responses and production are incomplete or incorrect.

J. The Department of Justice often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Department may make information supplied by you available to such agencies. Information you provide may be used in any federal, state, or foreign civil or criminal proceedings by the Department or other agencies.

K. Unless otherwise directed in the specifications, the applicable time period for the request shall be from **January 1, 2009,** through the date of your full and complete compliance with this subpoena.

L. You shall retain all documentary materials used in the preparation of responses to the specifications of this subpoena. The Department of Justice may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise.

M. If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Department of Justice's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with Trial Attorneys Joel Sweet at 202-532-4663 or Josh Burke at 202-353-2001. Any such modifications must be agreed to in writing.

N. Because postal delivery to the Department of Justice is subject to delay due to heightened security precautions, please use a courier service such as FedEx or UPS. Notice of your intended method of production should be given by telephone to Joel Sweet at 202-532-4663 at least five days prior to the return date.

O. All document requests should be responded to in accordance with the Instructions and Definitions provided herein.

II. DEFINITIONS

A. The word "document" has the same meaning as it does in Federal Rule of Civil Procedure 34(a)(1)(A), and is intended to be interpreted broadly to include electronically-stored information.

B. The terms "you," "your," and "Company" refer to Four Oaks Bank & Trust Co. and include corporate predecessors, merged predecessor corporations, parent corporations, past and present subsidiaries and affiliates, as well as current and former directors, officers, principals, partners, employees, agents, representatives, or other persons acting for or on behalf thereof, including, but not limited to, any otherwise independent accountant, investigator or consultant.

C. The terms "concerning," "relate to," "related to," and "relating to," mean discussing, describing, reflecting, embodying, memorializing, containing, constituting, including, identifying, stating, studying, reporting, commenting, evidencing, analyzing, setting forth, considering, recommending, concerning, or pertaining or being relevant to, in whole or in part.

D. The use of a singular shall be construed to include the plural and use of the plural shall be deemed to include the singular.

E. The words "and" and "or" shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification of the document requests all information that otherwise might be construed to be outside the scope of the specification.

F. The words "any" shall be construed to include the word "all," and the word "all" shall be construed to include the word "any."

G. The word "each" shall be construed to include the word "every," and "every" shall be construed to include the word "each."

H. The term "person" means any natural person, corporation, company, partnership, proprietorship, joint venture, firm, association, or other form of business or legal entity, and includes any affiliate, subsidiary, employee or representative thereof.

I. The term "Payment Processor" means and entity that performs any function of collecting, formatting, charging, originating, transmitting, or processing a consumer's payment for goods or services directly or indirectly through the use of any payment mechanism, including but not limited to the processing of Remotely-Created Check ("RCC") transactions, Remotely-Created Payment Order ("RCPO") transactions, automated clearing house ("ACH") transactions, mobile payments, and credit card transactions.

J. "Sale" means any sale, offer for sale, or attempt to sell, any goods or services to consumers for consideration.

K. The term "Merchant-Client" means any business or entity engaged, or purportedly engaged, in the Sale of goods or services directly or indirectly to consumers and that communicates with consumers using the Internet, telephones, or United States Postal System.

L. The term "Remotely-Created Check" ("RCC") means a check that is not created by the paying bank and that does not bear a signature applied, or purported to be applied, by the person on whose account the check is drawn. For purposes of this subpoena, the term RCC includes "demand drafts," "bank drafts," "bank checks," and "preauthorized drafts." For purposes of this subpoena, RCC specifically includes Remotely Created Payment Orders ("RCPO"). The term "account" as used herein is defined in Regulation CC, Availability of Funds and Collection of Checks, 12 CFR 229.2(a), as well as a credit or other arrangement that allows a person to draw checks that are payable by, through, or at a bank.

M. The term "Return" means any attempted debit transaction against a consumer's bank account that has been returned by the consumer's bank or the banking or payment system for any reason. For purposes of this subpoena, the term "Return" has the same meaning as a "chargeback."

N. "Return Rate" means the proportion (expressed as a percentage) of Return transactions relative to the total number of transactions originated for a given time period.

III. DOCUMENT REQUESTS

1. Documents sufficient to identify all Payment Processors for which you have originated RCC, RCPO, or ACH debit transactions against consumers' bank accounts.

2. All agreements (including all writings memorializing business terms) between you and all Payment Processors on behalf of which you originated RCC, RCPO, or ACH debit transactions against consumers' bank accounts.

3. Documents sufficient to identify the respective owners and addresses of all Payment Processors on behalf of which you have originated RCC, RCPO, or ACH debit transactions against consumers' bank accounts.

4. Documents sufficient to identify Payment Processors and/or Merchant-Clients that experienced a Return Rate of three (3) percent or greater in any one-month period.

5. For Payment Processors and Merchant Clients for which you have originated RCC, RCPO, or ACH debit transactions against consumers' accounts and that experienced a Return Rate of three (3) percent or greater in any one-month period, the complete due diligence file for that that entity and all of its customers (including but not limited to CIP information and documents identifying prior financial institution relationships).

6. For Payment Processors and Merchant Clients for which you have originated RCC, RCPO, or ACH debit transactions against consumers' accounts and that experienced a Return Rate of three (3) percent or greater in any one-month period, all Return summaries, databases, and/or reports.

7. All communications between or among you and: (a) any regulatory agency; (b) any law enforcement agency; (c) any financial institution; and/or (d) any consumer, concerning allegedly unauthorized debit transactions relating to Payment Processors and Merchant-Clients for which you have originated RCC, RCPO, or ACH debit transactions against consumers' accounts.

8. All communications between or among you and Payment Processors and Merchant-Clients for which you have originated RCC, RCPO, or ACH debit transactions against consumers' accounts concerning: (a) Returns; (b) inquiries by law enforcement or regulators; (c) consumer complaints; (d) allegations of fraud; and/or (e) allegations of unauthorized transactions.

9. Organizational charts reflecting your department(s) responsible for: (a) managing your business relationship(s) with Payment Processors; and (b) addressing complaints of unauthorized or fraudulently induced debit transactions against consumer bank accounts.

CERTIFICATE OF COMPLIANCE

I/We do hereby certify that a diligent search of the documentary material called for by the subpoena issued pursuant to 12 U.S.C. § 1833a(g)(1) has been made, and that all of the documentary material in the possession, custody or control of the person or entity to whom the subpoena is directed has been produced and made available at the time, place and manner specified. A list identifying all of the documents produced is attached.

Any documentary material otherwise responsive to this subpoena which has been withheld from production under a claim of privilege or for any other reason has been identified herein by (1) the date of the document, (2) the author(s), (3) the addressee(s), (4) the recipient(s), (5) the title, (6) the subject matter, (7) the purpose of the document, (8) its present custody, (9) such other information as is sufficient or necessary to identify the document, and (10) the nature of the privilege claimed. Any such withheld documentary material will be preserved until we receive notice from the United States Department of Justice that the investigation in furtherance of which the subpoena has been issued is no longer pending.

_____
Signature

_____
Title

Sworn to before this

_____ day of _____

_____
Notary Public

My commission expires: _____

UNITED STATES DEPARTMENT OF JUSTICE
CERTIFICATE OF COMPLIANCE
WITH THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

TO: [redacted]

FROM: Joel Sweet
Trial Attorney
U.S. Department of Justice
Consumer Protection Branch

To the extent that the records sought by the accompanying subpoena are subject to the Right to Financial Privacy Act of 1978 ("RFPA"), 12 U.S.C. §§ 3401 to 3422, because the exception set forth in 12 U S.C. § 3413(h)(l)(A) applies here given that this investigation is directed at financial institutions, I hereby certify that the applicable provisions of the RFPA have been complied with as to the subpoena issued by the Department of Justice pursuant to 12 U.S.C. § 1833a(g)(1) and as to subsequent subpoenas issued to you and requests for information from you in this matter.

Pursuant to the RFPA, good faith reliance upon this certificate relieves you and your employees and agents of any possible liability to the customer in connection with the disclosure of these financial records.

DATE: [redacted]

By: _____
JOEL SWEET

November 2013

Specifications for Production of ESI and Digitized ("Scanned") Images ("Production Specifications")

Collection of Electronically Stored Information (ESI)
Careful consideration should be given to the methodology, implementation and documentation of ESI collection to ensure that all responsive data and metadata are preserved in the collection process.

1. **Specification Modifications**
Any modifications or deviations from the Production Specifications may be done only with the express permission of the government. Any responsive data or documents that exist in locations or native forms not discussed in these Production Specifications remain responsive and, therefore, arrangements should be made with the government to facilitate their production.

2. **Production Format of ESI and Imaged Hard Copy**
Responsive ESI and imaged hard copy shall be produced in the format outlined below. All ESI, except as outlined below in sections 9 – 19, shall be rendered to type TIFF image format, and accompanied by a Concordance® Image Cross Reference file. All applicable metadata (see section 3 below) shall be extracted and provided in Concordance® load file format.

a. **Image File Format:** All images, paper documents scanned to images, or rendered ESI, shall be produced as 300 dpi single-page TIFF files, CCITT Group IV (2D Compression). Documents should be uniquely and sequentially Bates numbered with an endorsement burned into each image.
- All TIFF file names shall include the unique Bates number burned into the image.
- Each Bates number shall be a standard length, include leading zeros in the number, and be unique for each produced page.
- All TIFF image files shall be stored with the ".tif" extension.
- Images shall be OCR'd using a standard COTS products.
- All pages of a document or all pages of a collection of documents that comprise a folder or other logical grouping, including a box, shall be delivered on a single piece of media.
- No image folder shall contain more than 2000 images.

b. **Concordance® Image Cross Reference file:** Images should be accompanied by a Concordance® Image Cross Reference file that associates each Bates number with its corresponding single-page TIFF image file. The Cross Reference file should also contain the image file path for each Bates numbered page.
- Image Cross Reference Sample Format:

```
ABC00000001,OL,S,D:\DatabaseName\Images\001\ ABC00000001.TIF,Y,,,
ABC00000002,OL,S,D:\DatabaseName\Images\001\ ABC00000002.TIF,,,,
ABC00000003,OL,S,D:\DatabaseName\Images\001\ ABC00000003.TIF,,,,
ABC00000004,OL,S,D:\DatabaseName\Images\001\ ABC00000004.TIF,Y,,,
```

c. **Concordance® Load File:** Images should also be accompanied by a "text load file" containing delimited text that will populate fields in a searchable, flat database environment. The file should contain the required fields listed below in section 3.

- ASCII text delimited load files are defined using the following delimiters:

Field Separator	*^ or Code 094*
Text Qualifier	*| or Code 124*
Substitute Carriage Return or New Line	*® or Code 013*

Specifications for Production of ESI and Digitized ("Scanned") Images
("Production Specifications")

- The text file should also contain hyperlinks to applicable native files, such as Microsoft Excel or PowerPoint files.
- There should be one line for every record in a collection.
- The load file must contain a field map/key listing the metadata/database fields in the order they appear within the data file. For example, if the data file consists of a First Page of a Record (starting Bates), Last Page of a Record (ending Bates), Document ID, Document Date, File Name, and a Title, then the structure may appear as follows:

  |BEGDOC#|^|ENDDOC#|^|DOCID|^|DOCDATE|^|FILENAME|^|TITLE|

- The extracted/OCR text for each document should be provided as a separate single text file. The file name should match the BEGDOC# or DOCID for that specific record and be accompanied by the .txt extension.

3. **Required Metadata/Database Fields**

- A "✓" denotes that the indicated field should be present in the load file produced.
- "Other ESI" includes non-email or hard copy documents, including but not limited to data discussed in sections 6-9, and 12-19 below.

Field name	Field Description	Field Type	Field Value	Hard Copy	E-Mail	Other ESI
COMPANY	Company/Organization submitting data	Full Text	Unlimited	✓	✓	✓
BOX#	Submission/volume/box number	Note Text	10	✓	✓	✓
CUSTODIAN	Custodian(s)/Source(s) - format: Last, First or ABC Dept	Multi-Entry	Unlimited	✓	✓	✓
AUTHOR	Creator of the document	Note Text	160			✓
BEGDOC#	Start Bates (including prefix) - No spaces	Note Text	60	✓	✓	✓
ENDDOC#	End Bates (including prefix) - No spaces	Note Text	60	✓	✓	✓
DOCID	Unique document Bates # or populate with the same value as Start Bates (DOCID = BEGDOC#)	Note Text	60	✓	✓	✓
PGCOUNT	Page Count	Integer	10	✓	✓	✓
PARENTID	Parent's DOCID or Parent's Start Bates (for EVERY document including all Child documents)	Note Text	60	✓	✓	✓
ATTACHIDs	Child document list; Child DOCID or Child Start Bates	Multi-Entry	60	✓	✓	✓
ATTACHLIST	List of Attachment Bates numbers	Multi Entry	Unlimited		✓	✓
BEGATTACH	Start Bates number of first attachment	Note Text	60	✓	✓	✓
ENDATTACH	End Bates number of last	Note	60	✓	✓	✓

Specifications for Production of ESI and Digitized ("Scanned") Images
("Production Specifications")

Field name	Field Description	Field Type	Field Value	Hard Copy	E-Mail	Other ESI
	attachment	Text				
PROPERTIES	Privilege notations, Redacted, Document Withheld Based On Privilege	Multi-Entry	Unlimited	✓	✓	✓
RECORD TYPE	File, E-mail, Attachment, or Hard Copy	Note Text	60	✓	✓	✓
FROM	Author - format: Last name, First name	Note Text	160		✓	✓
TO	Recipient- format: Last name, First name	Multi-Entry	Unlimited		✓	✓
CC	Carbon Copy Recipients - format: Last name, First name	Multi-Entry	Unlimited		✓	✓
BCC	Blind Carbon Copy Recipients - format: Last name, First name	Multi-Entry	Unlimited		✓	✓
SUBJECT	Subject/Document Title	Note Text	Unlimited		✓	✓
CONVINDEX	E-mail system ID used to track replies, forwards, etc.	Note Text	Unlimited		✓	
DOCDATE	Document Date/Date Sent - Format YYYY/MM/DD	Date Keyed	YYYY/MM/DD			✓
BODY	E-mail body, Other Electronic Document Extracted text, or OCR	Full Text	Unlimited	✓	✓	✓
TIMESENT	Time e-mail was sent	Time	10		✓	
DATECRTD	Date Created	Date	YYYY/MM/DD		✓	✓
DATESVD	Date Saved	Date	YYYY/MM/DD		✓	✓
DATEMOD	Date Last Modified	Date Keyed	YYYY/MM/DD		✓	✓
DATERCVD	Date Received	Date	YYYY/MM/DD		✓	
DATEACCD	Date Accessed	Date	YYYY/MM/DD		✓	✓
FILESIZE	File Size	Note Text	10			✓
FILENAME	File name - name of file as it appeared in its original location	Full Text	Unlimited			✓
APPLICATION	Application used to create native file (e.g. Excel, Outlook, Word)	Note Text	160		✓	✓
FILE EXTENSION	Extension for the file (e.g. .doc; .pdf; .wpd)	Note Text	10		✓	✓
FILEPATH	Data's original source full folder path	Full Text	Unlimited		✓	✓
NATIVELINK	Current file path location to the native file	Full Text	Unlimited		✓	✓
FOLDERID	E-mail folder path (e.g. Inbox\Active) or Hard Copy container information (e.g.	Full Text	Unlimited	✓	✓	

Specifications for Production of ESI and Digitized ("Scanned") Images ("Production Specifications")

Field name	Field Description	Field Type	Field Value	Hard Copy	E-Mail	Other ESI
	Folder or binder name)					
PARAGRAPH	Subpoena/request paragraph number to which the document is responsive	Multi-Entry	Unlimited	✓	✓	✓
HASH	Hash value (used for deduplication or other processing) (e-mail hash values must be run with the e-mail and all of its attachments)	Note Text	Unlimited		✓	✓
MESSAGEHEADER	Email header. Can contain IP address	Full Text	Unlimited		✓	
ATTACHMCOUNT	Number of attachments to an email	Note Text	10		✓	
FILETYPE	Identifies the application that created the file	Note Text	160		✓	✓
COMMENTS	Identifies whether the document has comments associated with it	Note Text	10		✓	✓

4. **De-duplication, Near-Duplicate Identification, Email Conversation Threading and Other Culling Procedures**
De-duplication of exact copies within a custodian's data may be done, but all "filepaths" must be provided for each duplicate document. The recipient shall not use any other procedure to cull, filter, group, separate or de-duplicate, etc. (i.e., reduce the volume of) responsive material before discussing with and obtaining the written approval of the government. All objective coding (e.g., near dupe ID or e-mail thread ID) shall be discussed and produced to the government as additional metadata fields.

5. **Hidden Text**
All hidden text (e.g. track changes, hidden columns, mark-ups, notes) shall be expanded and rendered in the image file. For files that cannot be expanded the native files shall be produced with the image file.

6. **Embedded Files**
All non-graphic embedded objects (Word documents, Excel spreadsheets, .wav files, etc.) that are found within a file shall be extracted and produced. For purposes of production the embedded files shall be treated as attachments to the original file, with the parent/child relationship preserved.

7. **Image-Only Files**
All image-only files (non-searchable .pdfs, multi-page TIFFs, Snipping Tool [and other] screenshots, etc., as well as all other images that contain text) shall be produced with associated OCR text and metadata/database fields identified in section 3 for "Other ESI."

8. **Hard Copy Records**
   a. All hard copy material shall reflect accurate document unitization including all attachments and container information (to be reflected in the PARENTID, ATTACHID, BEGATTACH, ENDATTACH and FOLDERID). Unitization in this context refers to identifying and marking the boundaries of documents within the collection, where a document is defined as the smallest physical fastened unit within a bundle. (e.g., staples, paperclips, rubber bands, folders, or tabs in a binder.) The first document in the collection represents the parent document and all other documents will represent the children.

Specifications for Production of ESI and Digitized ("Scanned") Images
("Production Specifications")

b. All documents shall be produced in black and white TIFF format unless the image requires color. An image "requires color" when color in the document adds emphasis to information in the document or is itself information that would not be readily apparent on the face of a black and white image. Images identified as requiring color shall be produced as color 300 dpi single-page JPEG files.

c. All objective coding (e.g., document date or document author) should be discussed and produced to the government as additional metadata/database fields.

9. **Production of Spreadsheets and Presentation Files.** All spreadsheet and presentation files (e.g. Excel, PowerPoint) shall be produced in the unprocessed "as kept in the ordinary course of business" state (i.e., in native format). *See* section 18 below. The file produced should maintain the integrity of all source, custodian, application, embedded and related file system metadata. No alteration shall be made to file names or extensions for responsive native electronic files.

10. **Production of Email Repositories**
Email repositories, also known as email databases (e.g., Outlook .PST, Lotus .NSF, etc.), can contain a variety of items, including: messages, calendars, contacts, tasks etc. For purposes of production, responsive items shall include the "Email" metadata/database fields outlined in section 3, including but not limited to all parent items (mail, calendar, contacts, tasks, notes, etc.) and child files (attachments of files to email or other items) with the parent/child relationship preserved. Email databases from operating systems other than Microsoft Exchange shall be produced after consultation with and written consent of the government about the format for the production of such databases.

11. **Production of Items Originally Generated in E-Mail Repositories but Found and Collected Outside of Email Repositories, i.e., "Stand-alone" Items**
Any parent email or other parent items (e.g., calendar, contacts, tasks, notes, etc.) found and collected outside of email repositories (e.g., items having extensions like .MSG, .HTM, .MHT, etc.), shall be produced items with the "Email" metadata fields outlined in section 3, including but not limited to any attachments, maintaining the family (parent/child) relationship.

12. **Production of Instant Messenger (IM), Voicemail Data, Audio Data, Video Data, etc.**
The responding party shall identify, collect, and produce any and all data which is responsive to the requests which may be stored in audio or video recordings, cell phone/PDA/Blackberry/smart phone data, tablet data, voicemail messaging data, instant messaging, text messaging, conference call data, video/audio conferencing (e.g. GoTo Meeting, WebEx), and related/similar technologies. However, such data, logs, metadata or other files related thereto, as well as other less common but similar data types, shall be produced after consultation with and written consent of the government about the format for the production of such data.

13. **Social Media**
Prior to any production of responsive data from Social Media (e.g., Twitter, Facebook, Google+, LinkedIn, etc.)the producing party shall first discuss with the government the potential export formats before collecting the information.

14. **Productions of Structured Data**
Prior to any production of responsive data from a structured database (e.g., Oracle, SAP, SQL, MySQL, QuickBooks, etc.), the producing party shall first provide the database dictionary and a list of all reports that can be generated from the structured database. The list of reports shall be provided in native Excel (.xls) format.

15. **Productions of Structured Data from Proprietary Applications**
Prior to any production of structured data from proprietary applications (e.g., proprietary timekeeping, accounting, sales rep call notes, CRMs, SharePoint etc.) the producing party shall first provide the database

dictionary and a list of all reports that can be generated from the structured database. The list of reports shall be produced in native Excel (.xls) format.

16. **Production of Photographs with Native File or Digitized ESI**
Photographs shall be produced as single-page .JPG files with a resolution equivalent to the original image as it was captured/created. All .JPG files shall have extracted metadata/database fields provided in a Concordance® load file format as outlined in section 3 for "Other ESI."

17. **Images from which Text Cannot be OCR Converted**
An exception report shall be provided when limitations of paper digitization software/hardware or attribute conversion do not allow for OCR text conversion of certain images. The report shall include the electronic Bates, Document Id or Bates number(s) corresponding to each such image.

18. **Format of ESI from Non-PC or Windows-based Systems**
If responsive ESI is in non-PC or non-Windows-based Systems (e.g., Apple, IBM mainframes, and UNIX machines), the ESI shall be produced after discussion with and written consent of the government about the format for the production of such data.

19. **Production of Native Files (When Applicable Pursuant to These Specifications)**
Productions of native files, as called for in these specifications, shall have extracted metadata/database fields provided in a Concordance® load file format as defined in the field specifications for "Other ESI" as outlined in section 3.

    a. ESI shall be produced in a manner which is functionally useable by the government. The following are examples:
        - AutoCAD data, e.g., .DWG, .DXF, shall be processed/converted and produced as single-page .JPG image files and accompanied by a Concordance® image formatted load as described above. The native files shall be placed in a separate folder on the production media and linked by a hyperlink within the text load file.
        - GIS data shall be produced in its native format and be accompanied by a viewer such that the mapping or other data can be reviewed in a manner that does not detract from its ability to be reasonably understood.
        - Audio and video recordings shall be produced in native format and be accompanied by a viewer if such recordings do not play in a generic application (e.g., Windows Media Player).

20. **Bates Number Convention**
All images should be assigned Bates numbers before production to the government. The numbers should be "endorsed" (or "burned in") on the actual images. Native files should be assigned a single bates number for the entire file. The Bates number shall not exceed 30 characters in length and shall include leading zeros in the numeric portion. The Bates number shall be a unique name/number common to each page (when assigned to an image) or to each document (when assigned to a native file). If the government agrees to a rolling production, the naming/numbering convention shall remain consistent throughout the entire production. There shall be no spaces between the prefix and numeric value. If suffixes are required, please use "dot notation." Below is a sample of dot notation:

PREFIX0000001	PREFIX0000003
PREFIX0000001.001	PREFIX0000003.001
PREFIX0000001.002	PREFIX0000003.002

Specifications for Production of ESI and Digitized ("Scanned") Images ("Production Specifications")

21. **Media Formats for Storage and Delivery of Production Data**
Electronic documents and data shall be delivered on any of the following media:
    a. CD-ROMs and/or DVD-R (+/-) formatted to ISO/IEC 13346 and Universal Disk Format 1.02 specifications.
    b. External hard drives [USB 2.0 (or better) or eSATA, formatted to NTFS format specifications] or flash drives.
    c. Storage media used to deliver ESI shall be appropriate to the size of the data in the production.
    d. Media should be labeled with the case name, production date, Bates range, and producing party.

22. **Virus Protection and Security for Delivery of Production Data**
Production data shall be free of computer viruses. Any files found to include a virus shall be quarantined by the producing party and noted in a log to be provided to the government. Password protected or encrypted files or media shall be provided with corresponding passwords and specific decryption instructions. No encryption software shall be used without the written consent of the government.

23. **Compliance and Adherence to Generally Accepted Technical Standards**
Production shall be in conformance with standards and practices established by the National Institute of Standards and Technology ("NIST" at www.nist.gov), U.S. National Archives & Records Administration ("NARA" at www.archives.gov), American Records Management Association ("ARMA International" at www.arma.org), American National Standards Institute ("ANSI" at www.ansi.org), International Organization for Standardization ("ISO" at www.iso.org), and/or other U.S. Government or professional organizations.

24. **Read Me Text File**
All deliverables shall include a read me text file at the root directory containing: total number of records, total number of images/pages or files, mapping of fields to plainly identify field names, types, lengths and formats. The file shall also indicate the field name to which images will be linked for viewing, date and time format, and confirmation that the number of files in load files matches the number of files produced.

25. **Exception Log**
An Exception Log shall be included documenting any production anomalies utilizing the electronic Bates number (document id or control numbering) assigned during the collection, processing and production phases.

-XXX-

Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2012-A010
Issued: October 22, 2012
Subject: Risk Associated with Third-Party Payment Processors

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to provide guidance to financial institutions when filing Suspicious Activity Reports (SARs) on activities related to third-party payment processors ("Payment Processors"). This Advisory furthers the Department of the Treasury's broader efforts to protect the U.S. financial system from money laundering and terrorist financing.

Description of Third-Party Payment Processors

Non-Bank, or third-party, Payment Processors are financial institution customers that provide payment processing services to merchants and other business entities, typically initiating transactions on behalf of merchant clients that do not have a direct relationship with the Payment Processor's financial institution. Payment Processors use their own deposit accounts at a financial institution to process such transactions and sometimes establish deposit accounts at the financial institution in the names of their merchant clients. Traditionally, Payment Processors contracted primarily with U.S. retailers that had physical locations in the United States in order to help collect monies owed by customers on the retailers' transactions. These merchant transactions primarily included credit card payments, but also covered Automated Clearing House (ACH) debits and creating and depositing remotely created checks (RCCs) or "demand drafts." With the expansion of the Internet, Payment Processors may now service a variety of domestic and international merchants, including conventional retail and Internet-based establishments, prepaid travel, and Internet gaming enterprises.[1]

---

[1] *See* Federal Financial Institutions Examination Council (FFIEC) Exam Manual, pp. 239-242 (April 29, 2010). Although the FFIEC Exam Manual is issued by the federal banking regulators and relates to AML requirements applicable to banks, it contains guidance that may be of interest to all financial institutions that provide financial services to Payment Processors and MSBs.

Potential Red Flags for Illicit Use of Payment Processors[2]

Law enforcement has reported to FinCEN that recent increases in certain criminal activity have demonstrated that Payment Processors present a risk to the payment system by making it vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. Many Payment Processors provide legitimate payment transactions for reputable merchant clients. The risk profile of such entities, however, can vary significantly depending on the composition of their customer base. For example, Payment Processors providing consumer transactions on behalf of telemarketing and Internet merchants may present a higher risk profile to a financial institution than would other businesses. Telemarketing and Internet sales and RCC-related transactions tend to have relatively higher incidences of consumer fraud or potentially illegal activities.

Trends and indicators of suspicious activity associated with Payment Processors are provided by federal, state, and local law enforcement agencies, who work together under the Financial Fraud Enforcement Task Force's (FFETF) Consumer Protection Working Group. Suspicious activity as described below often is associated with Payment Processors engaged in improper or illegal conduct.

- *Fraud:* High numbers of consumer complaints about Payment Processors and/or merchant clients, and particularly high numbers of returns or charge backs (aggregate or otherwise), suggest that the originating merchant may be engaged in unfair or deceptive practices or fraud, including using consumers' account information to create unauthorized RCCs or ACH debits. Consumer complaints are often lodged with financial institutions, Payment Processors, merchant clients, consumer advocacy groups, online complaint Web sites or blogs, and governmental entities such as the Federal Trade Commission and state Attorneys General.

- *Accounts at Multiple Financial Institutions:* Payment Processors engaged in suspicious activity often maintain accounts at more than one financial institution. Similarly, they may move from one financial institution to another within a short period. Such Payment Processors also may use multiple financial institutions and maintain redundant banking relationships in recognition of the risk to the Payment Processor and merchant that a financial institution may recognize the suspicious activity and terminate the Payment Processor and/or merchant accounts. In addition, regulators and law enforcement have recognized an increased use of "check consolidation accounts"[3] by some Payment Processors.

---

[2] For additional information on fraudulent schemes identified by various government offices, refer to their websites and the DOJ FFETF site www.STOPFRAUD.GOV. Additional information on consumer fraud involving the use of Payment Processors and RCCs can be found at http://www.ftc.gov/.

[3] Returned Check Consolidation Accounts are legitimate and commonly used by commercial enterprises to facilitate processing of returned checks. Recently, however, some Payment Processors have used these accounts to establish separate deposit accounts to disposition their returned check items for the purpose of making it difficult for financial institutions to identify and evaluate "return/error" rates for the Payment Processor. In some instances, both the deposit account and the returned check consolidation account are held at the same institution but in different accounts. In other instances, the accounts are held at separate institutions. In either case, this account relationship structure severely inhibits a financial institution's ability to monitor and report suspicious activity.

Consolidation accounts can be used by Payment Processors to conceal high return or chargeback rates from originating financial institutions and regulators.

- *Money Laundering:* Criminals are continually looking for ways to launder illicit proceeds, including the proceeds of consumer fraud. Payment Processors can be used by criminals to mask illegal or suspicious transactions and to launder proceeds of crime. In addition, Payment Processors have been used to place illegal funds directly into a financial institution using ACH credit transactions originating from foreign sources.

- *Enhanced Risk:* There are potential risks associated with relationships with third-party entities, in particular foreign-located payment processors that process payments for telemarketers, online businesses, and other merchants. These relationships can pose increased risk to institutions and may require careful due diligence and monitoring.

- *Solicitation for Business:* Payment Processors engaged in suspicious activity have been known to solicit business relationships with distressed financial institutions in need of revenue and capital. Such Payment Processors may consider troubled financial institutions to be more willing to engage in higher-risk transactions. In some cases, Payment Processors also have committed to purchasing stock in these financial institutions to further induce the financial institution to provide banking services to high risk merchants. Often, the targeted financial institutions are smaller community banks that lack the infrastructure to properly manage or control a high-risk Payment Processor relationship. Fraudulent merchants also have been known to possess accounts through payment processors at large financial institutions.

- *Elevated rate of return of debit transactions due to unauthorized transactions:* Payment processors engaged in or complicit in suspicious activities may reflect a rate of return of debit items due to unauthorized transactions substantially higher than the average. Payment processors abused by criminals may show an acceptable rate (*i.e.* an average within normal parameters for the payment system involved) of returned items due to unauthorized transactions, calculated as a percentage of the processor's total transaction volume, but a much higher rate of returned items when the ratio is calculated on the traffic volume of individual originators.

Guidance

Financial institutions providing services to Payment Processors institutions may find it necessary to update their anti-money laundering programs.[4] Financial institutions should determine during thorough initial and ongoing due diligence, to the extent possible, whether external investigations or legal actions are pending against a Payment Processor or its owners and operators. Financial

---

[4] *See* footnote 1 above.

institutions also should determine whether Payment Processors have obtained all necessary state licenses, registrations, and approvals.[5]

Additionally, financial institutions may be required to file SARs if they know, suspect, or have reason to suspect that a Payment Processor has conducted a transaction involving funds derived from illegal activity, including, but not limited to, consumer fraud. A financial institution also may be required to file a SAR where it knows, suspects, or has reason to suspect that a Payment Processor has attempted to disguise funds derived from illegal activity, or has attempted to engage in transactions designed to evade regulations promulgated under the Bank Secrecy Act ("BSA") or that lack a legitimate business or apparent lawful purpose.[6]

To assist law enforcement in investigating and prosecuting possible criminal activity involving Payment Processors, FinCEN requests that, when reporting suspicious activity, financial institutions (1) check the appropriate box on the SAR form to indicate the type of suspicious activity, and (2) include the term "Payment Processor" in both the narrative portion and the subject occupation portions of the SAR.

Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).

---

[5] Financial Crimes Enforcement Network, "Advisory – Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States," (April 26, 2005), *available at* http://www.fincen.gov/statutes_regs/guidance/html/guidance04262005.html.

[6] *See, e.g.*, 31 CFR § 1020.320.

FDIC

Federal Deposit Insurance Corporation
550 17th Street NW, Washington, D.C. 20429-9990

Financial Institution Letter
FIL-3-2012
January 31, 2012

Payment Processor Relationships
Revised Guidance

Summary: Attached is revised guidance describing potential risks associated with relationships with third-party entities that process payments for telemarketers, online businesses, and other merchants (collectively "merchants"). These relationships can pose increased risk to institutions and require careful due diligence and monitoring. This guidance outlines certain risk mitigation principles for this type of activity.

Statement of Applicability to Institutions with Total Assets under $1 Billion: This guidance applies to all FDIC-supervised financial institutions that have relationships with third-party payment processors.

Distribution:
FDIC-Supervised Institutions

Suggested Routing:
Chief Executive Officer
Executive Officers
Compliance Officer
Chief Information Officer
BSA Officer

Related Topics:
Guidance on Payment Processor Relationships (FIL 127-2008, November 2008)
Consumer Protection, Compliance Risk, and Risk Management
FDIC Guidance for Managing Third-Party Risk (FIL 44-2008, June 2008)
FFIEC Handbook on Retail Payment Systems (February 2010)
FFIEC Handbook on Outsourcing Technology Services (June 2004)
FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual (April 2010)
Managing Risks in Third-Party Payment Processor Relationships (Summer 2011 Supervisory Insights Journal)

Attachment:
Revised Guidance on Payment Processor Relationships

Contacts:
Kathryn Weatherby, Examination Specialist (Fraud), Division of Risk Management Supervision, at kweatherby@fdic.gov or (703) 254-0469.

John Bowman, Review Examiner, Division of Depositor and Consumer Protection, at jbowman@fdic.gov or (202) 898-6574

Note:
FDIC Financial Institution Letters may be accessed from the FDIC's Web site at www.fdic.gov/news/news/financial/2012/index.html.

To receive Financial Institution Letters electronically, please visit http://www.fdic.gov/about/subscriptions/fil.html. Paper copies may be obtained through the FDIC's Public Information Center, 3501 Fairfax Drive, E-1002, Arlington, VA 22226 (877-275-3342 or 703-562-2200).

Highlights:

- Account relationships with third-party entities that process payments for merchants require careful due diligence, close monitoring, and prudent underwriting.
- Account relationships with high-risk entities pose increased risks, including potentially unfair or deceptive acts or practices under Section 5 of the Federal Trade Commission Act.
- Certain types of payment processors may pose heightened money laundering and fraud risks if merchant client identities are not verified and business practices are not reviewed.
- Financial institutions should assess risk tolerance in their overall risk assessment program and develop policies and procedures addressing due diligence, underwriting, and ongoing monitoring of high-risk payment processor relationships.
- Financial institutions should be alert to consumer complaints or unusual return rates that suggest the inappropriate use of personal account information and possible deception or unfair treatment of consumers.
- Financial institutions should act promptly when fraudulent or improper activities occur relating to a payment processor, including possibly terminating the relationship.
- Improperly managing these risks may result in the imposition of enforcement actions, such as civil money penalties or restitution orders.

Financial Institution Letter
FIL-3-2012
January 31, 2012

Revised Guidance on Payment Processor Relationships

The FDIC has recently seen an increase in the number of relationships between financial institutions and payment processors in which the payment processor, who is a deposit customer of the financial institution, uses its relationship to process payments for third-party merchant clients. Payment processors typically process payments either by creating and depositing remotely created checks (RCCs)—often referred to as "Demand Drafts"—or by originating Automated Clearing House (ACH) debits on behalf of their merchant customers. The payment processor may use its own deposit account to process such transactions, or it may establish deposit accounts for its merchant clients.

While payment processors generally effect legitimate payment transactions for reputable merchants, the risk profile of such entities can vary significantly depending on the make-up of their customer base. For example, payment processors that deal with telemarketing and online merchants[1] may have a higher risk profile because such entities have tended to display a higher incidence of consumer fraud or potentially illegal activities than some other businesses. Given this variability of risk, payment processors must have effective processes for verifying their merchant clients' identities and reviewing their business practices. Payment processors that do not have such processes can pose elevated money laundering and fraud risk for financial institutions, as well as legal, reputational, and compliance risks if consumers are harmed.

Financial institutions should understand, verify, and monitor the activities and the entities related to the account relationship. Although all of the core elements of managing third-party risk should be considered in payment processor relationships (e.g., risk assessment, due diligence, and oversight), managing this risk poses an increased challenge for the financial institution when there may not be a direct customer relationship with the merchant. For example, it may be difficult to obtain necessary information from the payment processor, particularly if a merchant is also a payment processor, resulting in a "nested" payment processor or "aggregator" relationship.

Financial institutions should ensure that their contractual agreements with payment processors provide them with access to necessary information in a timely manner. These agreements should also protect financial institutions by providing for immediate account closure, contract termination, or similar action, as well as establishing adequate reserve requirements to cover anticipated charge backs. Accordingly, financial institutions should perform due diligence and account monitoring appropriate to the risk posed by the payment processor and its merchant

[1] Examples of telemarketing, online businesses, and other merchants that may have a higher incidence of consumer fraud or potentially illegal activities or may otherwise pose elevated risk include credit repair services, debt consolidation and forgiveness programs, online gambling-related operations, government grant or will-writing kits, payday or subprime loans, pornography, online tobacco or firearms sales, pharmaceutical sales, sweepstakes, and magazine subscriptions. This list is not all-inclusive.

base. Risks associated with this type of activity are further increased if neither the payment processor nor the financial institution performs adequate due diligence on the merchants for which payments are originated. Financial institutions are reminded that they cannot rely solely on due diligence performed by the payment processor. The FDIC expects a financial institution to adequately oversee all transactions and activities that it processes and to appropriately manage and mitigate operational risks, Bank Secrecy Act (BSA) compliance, fraud risks, and consumer protection risks, among others.

Potential Risks Arising from Payment Processor Relationships

Deposit relationships with payment processors expose financial institutions to risks not customarily present in relationships with other commercial customers. These include increased operational, strategic, credit, compliance, and transaction risks. In addition, financial institutions should consider the potential for legal, reputational, and other risks, including risks associated with a high or increasing number of customer complaints and returned items, and the potential for claims of unfair or deceptive practices. *Financial institutions that fail to adequately manage these relationships may be viewed as facilitating a payment processor's or merchant client's fraudulent or unlawful activity and, thus, may be liable for such acts or practices.* In such cases, the financial institution and responsible individuals have been subject to a variety of enforcement and other actions. Financial institutions must recognize and understand the businesses and customers with which they have relationships and the liability risk for facilitating or aiding and abetting consumer unfairness or deception under Section 5 of the Federal Trade Commission Act.[2]

Financial institutions should be alert for payment processors that use more than one financial institution to process merchant client payments or that have a history of moving from one financial institution to another within a short period. Processors may use multiple financial institutions because they recognize that one or more of the relationships may be terminated as a result of suspicious activity.

Financial institutions should also be on alert for payment processors that solicit business relationships with troubled financial institutions in need of capital. In such cases, payment processors will identify and establish relationships with troubled financial institutions because these financial institutions may be more willing to engage in higher-risk transactions in exchange for increased fee income. In some cases, payment processors have also committed to purchasing stock in certain troubled financial institutions or have guaranteed to place a large deposit with the financial institution, thereby providing additional, much-needed capital. Often, the targeted financial institutions are smaller, community banks that lack the infrastructure to properly manage or control a third-party payment processor relationship.

[2] Under Section 8 of the Federal Deposit Insurance Act, the FDIC has authority to enforce the prohibitions against Unfair or Deceptive Acts or Practices (UDAP) in the Federal Trade Commission Act. UDAP violations can result in unsatisfactory Community Reinvestment Act ratings, compliance rating downgrades, restitution to consumers, and the pursuit of civil money penalties.

Financial institutions also should be alert to an increase in consumer complaints about payment processors and/or merchant clients or an increase in the amount of returns or charge backs, all of which may suggest that the originating merchant may be engaged in unfair or deceptive practices or may be inappropriately obtaining or using consumers' personal account information to create unauthorized RCCs or ACH debits. Consumer complaints may be made to a variety of sources and not just directly to the financial institution. They may be sent to the payment processor or the underlying merchant, or directed to consumer advocacy groups or online complaint Web sites or blogs. Financial institutions should take reasonable steps to ensure they understand the type and level of complaints related to transactions that it processes. Financial institutions should also determine, to the extent possible, if there are any external investigations of or legal actions against a processor or its owners and operators during initial and ongoing due diligence of payment processors.

Financial institutions should act promptly to minimize possible consumer harm, particularly in cases involving potentially fraudulent or improper activities relating to activities of a payment processor or its merchant clients. Appropriate actions include filing a Suspicious Activity Report,[3] requiring the payment processor to cease processing for a specific merchant, freezing certain deposit account balances to cover anticipated charge backs, and/or terminating the financial institution's relationship with the payment processor.

Risk Mitigation

Financial institutions should delineate clear lines of responsibility for controlling risks associated with payment processor relationships. Controls may include enhanced due diligence; effective underwriting; and increased scrutiny and monitoring of high-risk accounts for an increase in unauthorized returns, charge backs, suspicious activity, and/or consumer complaints. Implementing appropriate controls for payment processors and their merchant clients can help identify payment processors that process items for fraudulent telemarketers, online scammers, or other unscrupulous merchants and help ensure that the financial institution is not facilitating these transactions. Appropriate oversight and monitoring of these accounts may require the involvement of multiple departments, including information technology, operations, BSA/anti-money laundering (AML), and compliance.

Due Diligence and Underwriting

Financial institutions should implement policies and procedures designed to reduce the likelihood of establishing or maintaining inappropriate relationships with payment processors used by unscrupulous merchants. Such policies and procedures should outline the bank's thresholds for unauthorized returns, the possible actions that can be taken against payment processors that exceed these standards, and methods for periodically reporting such activities to the bank's board of directors and senior management.

[3] The U.S. Department of Treasury's Regulation 31 (CFR 103.18) requires that every federally supervised banking organization file a SAR when the institution detects a known or suspected violation of federal law. Part 353 of the FDIC's Rules and Regulations addresses SAR filing requirements and makes them applicable to all state-chartered financial institutions that are not members of the Federal Reserve System.

As part of such policies and procedures, financial institutions should develop a processor approval program that extends beyond credit risk management. This program should include a due diligence and underwriting policy that, among other things, requires a background check of the payment processor, its principal owners, and its merchant clients. This will help validate the activities, creditworthiness, and business practices of the payment processor, as well as identify potential problem merchants. Payment processors may also process transactions for other payment processors, resulting in nested payment processors or aggregator relationships. The financial institution should be aware of these activities and obtain data on the nested processor and its merchant clients. Nested processors and aggregator relationships pose additional challenges as they may be extremely difficult to monitor and control; therefore, risk to the institution is significantly elevated in these cases.

Controls and due diligence requirements should be robust for payment processors and their merchant clients. At a minimum, the policies and procedures should authenticate the processor's business operations and assess the entity's risk level. An assessment should include:

- Identifying the major lines of business and volume for the processor's customers;
- Reviewing the processor's policies, procedures, and processes to determine the adequacy of due diligence standards for new merchants;
- Reviewing corporate documentation, including independent reporting services and, if applicable, documentation on principal owners;
- Reviewing the processor's promotional materials, including its Web site, to determine the target clientele;[4]
- Determining if the processor re-sells its services to a third party that may be referred to as an agent or provider of "Independent Sales Organization opportunities" or a "gateway arrangement"[5] and whether due diligence procedures applied to those entities are sufficient;
- Visiting the processor's business operations center;
- Reviewing appropriate databases to ensure that the processor and its principal owners and operators have not been subject to law enforcement actions; and,
- Determining whether any conflicts of interest exist between management and insiders of the financial institution.

[4] See footnote 1 for examples of potentially high-risk areas.

[5] An Independent Sales Organization is an outside company contracted to procure new merchant relationships. Gateway arrangements are similar to Internet service providers that sell excess computer storage capacity to third parties, who in turn distribute computer services to other individuals unknown to the provider. The third party would make decisions about who would be receiving the service, although the provider would be responsible for the ultimate storage capacity.

Financial institutions should require that payment processors provide information on their merchant clients, such as the merchant's name, principal business activity, location, and sales techniques. The same information should be obtained if the merchant uses sub-merchants (often called "affiliates"). Additionally, financial institutions should verify directly, or through the payment processor, that the originator of the payment (i.e., the merchant) is operating a legitimate business. Such verification could include comparing the identifying information with public record, fraud databases, and a trusted third party, such as a consumer reporting agency or consumer advocacy group, and/or checking references from other financial institutions. The financial institution should also obtain independent operational audits of the payment processor to assess the accuracy and reliability of the processor's systems. The more the financial institution relies on the payment processor for due diligence and monitoring of its merchant client without direct financial institution involvement and verification, the more important it is to have an independent review to ensure that the processor's controls are sufficient and that contractual agreements between the financial institution and the third-party payment processor are honored.

Ongoing Monitoring

Financial institutions that initiate transactions for payment processors should implement systems to monitor for higher rates of returns or charge backs and/or high levels of RCCs or ACH debits returned as unauthorized or due to insufficient funds, all of which often indicate fraudulent activity. This would include analyzing and monitoring the adequacy of any reserve balances or accounts established to continually cover charge-back activity.

Financial institutions are required to have a BSA/AML compliance program and appropriate policies, procedures, and processes for monitoring, detecting, and reporting suspicious activity. However, nonbank payment processors generally are not subject to BSA/AML regulatory requirements, and therefore some payment processors are more vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions. The FFIEC BSA/AML Examination Manual urges financial institutions to effectively assess and manage risk associated with third-party payment processors. As a result, a financial institution's risk mitigation program should include procedures for monitoring payment processor information, such as merchant data, transaction volume, and charge-back history.

Consumer complaints and/or high rates of return may be an indicator of unauthorized or illegal activity. As such, financial institutions should establish procedures for regularly surveying the sources of consumer complaints that may be lodged with the payment processor, its merchant clients or their affiliates, or on publicly available complaint Web sites and/or blogs. This will help the institutions identify processors and merchants that may pose greater risk.

Similarly, financial institutions should have a formalized process for periodically auditing their third-party payment processing relationships; including reviewing merchant client lists and confirming that the processor is fulfilling contractual obligations to verify the legitimacy of its merchant clients and their business practices.

Conclusion

The FDIC recognizes that financial institutions provide legitimate services for payment processors and their merchant clients. However, to limit potential risks, financial institutions should implement risk mitigation policies and procedures that include oversight and controls appropriate for the risk and transaction types of the payment processing activities. At a minimum, Board-approved policies and programs should assess the financial institution's risk tolerance for this type of activity, verify the legitimacy of the payment processor's business operations, determine the character of the payment processor's ownership, and ensure ongoing monitoring of payment processor relationships for suspicious activity, among other things. Adequate routines and controls will include sufficient staffing with the appropriate background and experience for managing third-party payment processing relationships of the size and scope present at the institution, as well as strong oversight and monitoring by the board and senior management. Financial institutions should act promptly if they believe fraudulent or improper activities potentially resulting in consumer harm have occurred related to activities of a payment processor or its merchant clients, in accordance with their duties under BSA/AML policies and procedures, as well as under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive acts and practices.

Sandra L. Thompson
Director
Division of Risk Management Supervision

Mark Pearce
Director
Division of Depositor and Consumer Protection

Office of the
Comptroller of the Currency
U.S. Department of the Treasury

OCC 2008-12

Subject: Payment Processors
Date: April 24, 2008

To: Chief Executive Officers, Chief Risk Officers and Compliance Officers of All National Banks, Federal Branches and Agencies, Technology Service Providers, Department and Division Heads, and All Examining Personnel

Description: Risk Management Guidance

Purpose

This bulletin presents guidance to national banks for due diligence, underwriting, and monitoring of entities that process payments for telemarketers and other merchant clients. As detailed in several OCC issuances, certain merchants, such as telemarketers, pose a higher risk than other merchants and require additional due diligence and close monitoring. This bulletin supplements, but does not replace, existing guidance related to Automated Clearing House (ACH) risk management, merchant processing, and remotely-created checks (RCCs).

Background

The OCC has seen a variety of relationships between banks and processors in which the processor uses its bank relationship to process payments for merchant clients. Often the processor uses a bank account as the vehicle to conduct such payment processing. For example, a processor may be a bank customer that deposits into its account RCCs generated on behalf of merchant clients. A processor may also act as a third-party sender of ACH transactions, originating debits for its merchant clients through its customer relationship with the bank. In either case, the bank often has no direct customer relationship with the merchant. Risks are heightened when neither the processor nor the bank performs adequate due diligence on the merchants for which they are originating payments.

When a bank has a relationship with a processor, it is exposed to risks that may not be present in relationships with other commercial customers. The bank encounters strategic, credit, compliance, transaction, and reputation risks in these relationships. Banks have two distinct areas of responsibility to control those risks. The first is due diligence and underwriting, and the second is monitoring these high-risk accounts for high levels of unauthorized returns and for suspicious or unusual patterns of activity. Proper initial due diligence, effective underwriting, and ongoing account monitoring are critical for bank safety and soundness and consumer protection. Banks should implement these controls to reduce the likelihood of establishing or maintaining an inappropriate relationship with a processor through which unscrupulous merchants can gain access to consumers' bank accounts.

Banks should also consider carefully the legal, reputation, and other risks presented by relationships with processors including risks associated with customer complaints, returned items, and potential unfair or deceptive practices.[1] Banks that do not have the appropriate controls to address the risks in these relationships may be viewed as facilitating a processor's or its merchant client's fraud or other unlawful activity. Banks should be alert for processors that use more than one bank to process payments for merchant clients and should subject such processors to great scrutiny. Processing through multiple banks may be a signal that the processor recognizes a risk that one or more of these processing relationships may be terminated as a result of suspicious, fraudulent, or other unlawful conduct.[2]

Risk Management: Effective Due Diligence, Underwriting, and Monitoring

The OCC has provided guidance to national banks regarding relationships with processors. For example, banks must implement a due diligence and underwriting policy that, among other things, requires an initial background check of the processor and its underlying merchants to support the validity of the processor's and merchants' businesses, their creditworthiness, and business practices.[3] Moreover, the OCC has also provided banks detailed procedures for merchant underwriting and review, as well as for fraud monitoring.[4] Banks should review carefully the validity and creditworthiness of all processors and merchants. Controls should be more rigorous for higher-risk processors and merchants (e.g., telemarketers). Although some processors may process transactions for reputable telemarketing merchants, those merchants in aggregate have displayed a much higher incidence of unauthorized returns or chargebacks, which is often indicative of fraudulent activity.

Due diligence, underwriting and account monitoring are especially important for banks in which processors deposit RCCs and through which processors initiate ACH transactions for their merchant clients. Banks should be alert to processors' merchant clients that obtain personal bank account information inappropriately. The merchant may have misused the customer information to facilitate the creation of an unauthorized RCC or ACH debit file by the processor.[5] To ensure effective risk management, banks that initiate transactions for processors should require the processor to provide information on their merchant clients such as the merchant's name, principal business activity, and geographic location.[6] Banks should verify directly, or through the processor, that the originator of the payment (*i.e.* the merchant) is operating a legitimate business. Such verification could include comparing the identifying information against public record databases and fraud and bad check databases, comparing the identifying information with information from a trusted third party, such as a credit report from a consumer reporting agency, or checking references from other financial institutions. With respect to account monitoring, a bank should not accept high levels of returns[7] on the basis that the processor has provided collateral or other security to the bank.

By implementing the appropriate controls over processors and their merchant clients, a bank should be able to identify those processors that process for fraudulent telemarketers or other unscrupulous merchants and to ensure that the bank is not facilitating these transactions. In the

event a bank identifies fraudulent or other improper activity with a processor or a specific merchant client of the processor, the bank should take immediate steps to address the problem, including filing a Suspicious Activity Report when appropriate, terminating the bank's relationship with the processor, or requiring the processor to cease processing for that specific merchant.

Banks are required to have Bank Secrecy Act/Anti-Money Laundering (BSA/AML) compliance programs and appropriate policies, procedures, and processes to monitor and identify unusual activity. Additionally, the FFIEC BSA/AML Examination Manual reiterates the OCC's expectation that banks effectively assess and manage their risks with respect to third-party processors. Processors generally are not subject to BSA/AML regulatory requirements. As a result, some processors may be vulnerable to money laundering, identity theft, fraud schemes, and illicit transactions or transactions prohibited by the Office of Foreign Assets Control. The bank's risk management program should include procedures for monitoring processor information such as merchant data, transaction volume, and charge-back history.[8]

Conclusion

The OCC supports national banks' participation in payment systems to serve the needs of legitimate processors and the customers of such processors and to diversify sources of revenue. However, to limit potential risk to banks and consumers, banks should ensure implementation of risk management programs that include appropriate oversight and controls commensurate with the risk and complexity of the activities. At a minimum, bank programs should verify the legitimacy of the processor's business operations, assess the bank's risk level, and monitor processor relationships for activity indicative of fraud.

Additional Information

For additional information related to managing the risks associated with retail payment activities please refer to:

- OCC Bulletin 2006-39, ACH Activities: Risk Management Guidance.
- The "Merchant Processing" booklet of the *Comptroller's Handbook*.
- OCC Bulletin 2006-13, Amendments to Regulation CC and J.
- OCC Bulletin 2001-47, Third-Party Relationships: Risk Management Principles.
- The "Outsourcing Technology Services" booklet of the *Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook*.
- The "Retail Payment Systems" booklet of the *FFIEC IT Examination Handbook*.
- The *FFIEC Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual*.

Please direct any questions or comments to the Operational Risk Policy Division at (202) 874-5190.

Mark L. O'Dell
Deputy Comptroller for Operational Risk

---

[1] See 15 USC 45. See also OCC Advisory Letter 2002-3, Guidance on Unfair or Deceptive Acts or Practices.

[2] See, e.g., OCC Bulletin 2006-39, p.10.

[3] See the "Merchant Processing" booklet of the *Comptroller's Handbook*, pp. 24-28, 34; The FFIEC's Bank Secrecy Act/Anti-Money Laundering Examination Manual, Third Party Payment Processors; and OCC Bulletin 2006-39, pp. 5, 10-11.

[4] See the "Merchant Processing" booklet of the *Comptroller's Handbook*, pp. 24-28.

[5] Though the Merchant Processing booklet of the Comptroller's Handbook addresses directly merchant card acquiring, its principles and most of the procedures outlined in the handbook are also applicable to the processing of other payment instruments, including RCCs and ACH transactions. See, e.g., OCC Bulletin 2006-39, footnote 7 and accompanying text.

[6] See OCC Bulletin 2006-39. A background check on the principal business owners supplements the underwriting of the merchant client. It is not uncommon for unscrupulous owners to use multiple business entities to avoid detection.

[7] Generally, a bank should not accept high levels of returns regardless of the return reason. High levels of RCCs or ACH debits returned for insufficient funds can be an indication of fraud.

[8] FFIEC BSA/AML Examination Manual, p. 219 (Third Party Payment Processors). See also OCC Bulletin 2006-39.

Mr. ISSA. Thank you.

In this document, which I am——

Mr. BACHUS. Now we will start your time.

Mr. ISSA. Thank you. Thank you. That would be great.

Mr. BACHUS. Or are you still introducing your——

Mr. ISSA. I am done introducing.

Mr. BACHUS. Okay.

Mr. ISSA. But in this document it, which I am told there is at least 50 subpoenas identical to this other than the name, are you familiar with this document?

Mr. DELERY. I believe so. I certainly am familiar with ones like that. I am not sure about that one.

Mr. ISSA. We know that 50 subpoenas were served that were substantially similar or identical except for name. How many subpoenas did you serve similar to the one that you believe I have got here?

Mr. DELERY. Well, again, I do think some of the documents have indicated in the neighborhood of 50, which again, were not all necessarily identical.

Mr. ISSA. Well, let's go through them. You named one company in which you had, prior to the serving of the subpoena, allegations of wrongdoing and complaints by customers. Is that correct? I mean, that is a standard to go looking, is that you have allegations of a bank doing things wrong, and that would be a reasonable reason.

Mr. DELERY. Yes.

Mr. ISSA. You had that in the case of Four Oaks, right?

Mr. DELERY. Again, that certainly was the basis for the case. And as to all of the subpoenas——

Mr. ISSA. Well, you are not allowed to go on fishing expeditions just generally and harass banks, are you?

Mr. DELERY. In each of the——

Mr. ISSA. No, no, no, that is a question. You are not allowed to go and just harass for the sake of—you can't send subpoenas to every single bank. Let me rephrase that. The statute allows to you do it, but that is not your practice. Is that correct?

Mr. DELERY. That is correct. And in this case there was a reasonable suspicion, a reasonable basis for each of the subpoenas that were issued.

Mr. ISSA. Then since these cases have come to a close without prosecution, would you provide to us the reasonable suspicion in the case of the—or at least an outline of them—in the case of these 50 subpoenas served?

Mr. DELERY. I think, Congressman, many of them relate to ongoing investigations.

Mr. ISSA. Obviously, only the closed cases.

Mr. DELERY. And so we can certainly look at the request. As I indicated earlier, we have a number of open——

Mr. ISSA. Okay. Well, let's go through this. It has earlier been testified that in fact these were just subpoenas and they were not intended to intimidate or cause people to change their behavior. Is that right?

Mr. DELERY. Right, they were intended to get information from institutions that we believed had evidence of fraud.

Mr. ISSA. So now listed in those evidence of fraud, in addition to Ponzi schemes, which are criminal, period, and if somebody knew about a Ponzi scheme, it is inherently a crime, right?

Mr. DELERY. That is my understanding, yes.

Mr. ISSA. There is credit card repair services, debt consolidation, online gaming, government grants, or will-writing kits, payday and subprime. Threw in pornography, I thought that was good, that pornography is inherently something that you should tell people about. Online tobacco, is that unlawful?

Mr. DELERY. I am not sure what document you are looking at.

Mr. ISSA. I am looking at the examples that are in your subpoena. Your subpoena includes an attachment of a financial institution letter. Your subpoena, all 50 of your subpoenas included an intimidating list of firearm sales, pharmaceutical sales, sweepstakes, magazine subscriptions, online tobacco. You included FDIC high-risk list in there that includes a series of lawful businesses. Are you aware of that?

Mr. DELERY. So the guidance was attached——

Mr. ISSA. Sir, were you aware of that?

Mr. DELERY. I am aware that the guidance was attached to, my understanding, is not all of the subpoenas.

Mr. ISSA. Oh, okay. Well, we would love to have all of them.

In testimony before the House Financial Services Committee on Tuesday you repeatedly disclaimed any involvement in the FDIC high-risk merchant guidance. Now, isn't is true that—assuming that this is a correct document, we would like you to authenticate it here today, and we will provide it to you—this in fact shows that what you said in Financial Services just isn't so? You included the guidance. You said in Financial Services you didn't, and I quote, you repeatedly disclaimed any involvement with the FDIC high-risk merchant guidance, and then you include it in your subpoena.

How is somebody supposed to think that you didn't participate in promoting this and you put it into a subpoena that threatens the hell out of a small community bank or credit union? How do you reconcile that?

Mr. DELERY. So I would be happy to answer that question, Congressman.

Mr. ISSA. I would be happy to get an answer to that one.

Mr. DELERY. The guidance that was attached is guidance that the FDIC provided. It discusses in general terms the risks that third-party payment processors can present——

Mr. ISSA. That is fine. But didn't by inclusion of that guidance, didn't you in fact by inclusion associate yourself with the position of the FDIC? And didn't you on Tuesday say just the opposite in the Financial Services Committee? So are you going to correct the record at Financial Services to disclose that in fact you had associated yourself, you had included the guidance, and you did in fact essentially team yourself with the FDIC for guidance that would say, credit card repair, payday subprime, online tobacco sales, firearm sales, ammunition sales, pharmaceutical sales, these are high risk, in a document you attached and then said that you are not associating yourself with the FDIC? Which is true?

Mr. DELERY. Congressman, I don't think that that is a complete description of what I said on Tuesday. Our policy in this area——

Mr. ISSA. Did you sign the subpoenas?

Mr. DELERY. Yes.

Mr. ISSA. I find your signature on the subpoena.

Mr. DELERY. Yes.

Mr. ISSA. You signed the subpoena. It had——

Mr. JOHNSON. Mr. Chairman?

Mr. ISSA. I just want to make one point and I will close.

Mr. JOHNSON. I just don't want you to badger the witness.

Mr. ISSA. I don't want to badger, I just want to make a point in closing, because I believe the Financial Services Committee has a real reason to relook at this gentleman's testimony. He signed the subpoenas, he attached the subpoenas, specific allegations of high risk, and then before the Financial Services Committee he testified that in fact he was not associated, and yet it was stapled to it.

It is not common for subpoenas to have other documents and fliers stapled to them. Generally, a subpoena isn't owned by the issuing party.

So I appreciate the gentleman yielding me the additional time. I thank the Chairman for his indulgence. And I will have a copy of this brought to the gentleman to refresh his memory of what he signed.

Mr. BACHUS. Thank you.

Mr. JOHNSON. Well, I think it is only fair that he see the document that you are seeking to——

Mr. ISSA. And we are going to give a copy to him right now. But he signed it. I figure he saw it once.

Mr. BACHUS. He signed it.

Mr. JOHNSON. He still deserves to see it.

Mr. BACHUS. Well, but he signed it. I mean, he signed it.

Mr. JOHNSON. You mischaracterized what he signed, if he signed it, and you are drawing conclusions from it that are probably——

Mr. ISSA. Mr. Chairman, the gentleman may be right. I would like unanimous consent for the Attorney General to have the opportunity to see it.

Mr. BACHUS. Let me ask, is that it right there?

Do you want to see it?

I guess we could ask him if in fact is familiar with that.

Mr. JOHNSON. Because he has not been able to explain one answer in response to the questions.

Mr. BACHUS. Do you have a motion? I mean, we will give our witness the opportunity.

Are you familiar with that document?

Mr. DELERY. Yes, Mr. Chairman. I think it is one of the subpoenas, as I indicated.

Mr. BACHUS. Well, just by way of giving you an opportunity to explain, did you sign that subpoena?

Mr. DELERY. Yes.

Mr. BACHUS. Okay. And is that list of high-risk categories, is that attached to the subpoena?

Mr. DELERY. There is a footnote in one of the attachments to the subpoena that makes reference to certain industries or businesses that the FDIC may consider to be high risk. And I think that goes to the point of the discussion on Tuesday. I think if you look at the overall discussion on Tuesday, what I explained was that our basis

for issuing the subpoenas was to pursue specific evidence of unlawful conduct, based on fraud against consumers, that we were not seeking to target any industry or business acting lawfully.

And in fact I also said that the participation of a financial institution with any particular industry, whether on a high-risk list or otherwise, was not a basis for an action that we were pursuing. So I think that is what I was saying the other day, on Tuesday.

Mr. BACHUS. Actually, if you look on page 1 of that attachment, it not only refers to it, it lists different payday loans, tobacco sales, firearm sales, pharmaceutical sales, magazine subscriptions, sweepstakes. It actually narrows it to those categories. So it actually is a more concise list than the FDIC's list.

Mr. DELERY. I am not sure, Mr. Chairman, which page you are looking at on this point.

Mr. BACHUS. The revised guidance on payment processor relationships, dated January 31st, 2012.

Mr. DELERY. Yeah. I think I am looking at that. That is part of the FDIC——

Mr. BACHUS. It does say payday or subprime loans, pornography. You are not equating the two, are you?

Mr. DELERY. No.

Mr. BACHUS. Online tobacco or firearm sales, pharmaceutical sales.

Mr. DELERY. No, Congressman. No, Mr. Chairman. I think what we have said is that participating in any particular line of business is not evidence of fraud. That is not how we are——

Mr. BACHUS. Do you think it was appropriate to attach a list to your subpoena?

Mr. DELERY. I think that, as I understand it, the purpose of the attachment was to respond to questions about the issues and the potential for fraud that third-party payment party processors provide.

I will come back.

Mr. JOHNSON. We will have a second round.

Mr. BACHUS. Yeah, absolutely. And we will give everybody plenty of time. But firearm sales, I mean, that is——

Mr. ISSA. Mr. Chairman, one might say beauty is in the eye of the beholder. And this Administration considers firearm sales, ammunition, as somewhat less beautiful than others. But that is the reason that this whole high-risk list under Operation Choke Point is so problematic, it makes ideological decisions of what is high risk, rather than economic.

Mr. JOHNSON. I would like to ask this witness whether or not it is true that this list that we are talking about of potentially illicit activities that banking institutions should be aware of——

Mr. BACHUS. Yeah, yeah, that is right. Illicit activities, that is a good word. Payday lending is illicit.

Mr. JOHNSON [continuing]. Whether or not that list is something that predates the Obama administration. Isn't it a fact that the FDIC list of activities that is the subject of this discussion is a product of a prior Administration?

Mr. BACHUS. I can answer that. It was 2011, which was 3 years into the Obama administration.

Mr. ISSA. Mr. Chairman, for the record, in 2008 there was a warning on high risk, but there was no specificity. They didn't name any entity. So it is very different to say beware of high risk.

Mr. BACHUS. And they didn't subpoena.

Mr. ISSA. They didn't subpoena. And if you a 50 percent return rate, that is high risk.

Mr. BACHUS. Let me say this, we are going to have a second round. So we will go to Mr. Jeffries.

Mr. JOHNSON. Well, for the record, the OCC on September the 1st of 2006 stated specifically listed industries associated with high volumes of unauthorized returns in a guidance document.

Mr. BACHUS. The Justice Department?

Mr. JOHNSON. The OCC. And so these are not Justice Department guidelines, even though they were referred to in the subpoena.

Mr. BACHUS. But what we are talking about here is a subpoena that cost hundreds of thousands of dollars to comply with on occasions. And you are all familiar with the term, in fact anyone that has ever served on Financial Services knows the term de-risking. That is a term that is used by the Justice Department. De-risking names that companies like to avoid risk. If you send them a subpoena and you list companies that are "risky" firearm sales——

Mr. JOHNSON. Not companies, but industries.

Mr. BACHUS. Industries. They are going to avoid risk by jettisoning those customers. We all know that. You know that.

Mr. JOHNSON. If there is any indicia of illegal activity that would derive from their actions.

Mr. BACHUS. Well, getting a subpoena and saying you are investigating fraud is a pretty, pretty strong method.

Mr. JOHNSON. If you have a reasonable suspicion that a fraud has been committed, Mr. Chairman, I think that that is what our——

Mr. BACHUS. And one thing, Mr. Delery, one reason that we are so concerned about this, normally you go to a court and you get a subpoena, a court approves it. This is one of the few cases under FIRREA, as you know, where you don't have to get the court's approval. You can launch these things and the burden of proof is very low.

Mr. ISSA. Mr. Chairman, you are exactly right, and I think Mr. Johnson made the point very well, in that if there is evidence of fraud, which apparently there may have been in one case, then the subpoena would follow, if you will, almost the ordinary course, even though it doesn't need a judge.

In the case of issuing 50, if there is not a specific allegation but rather a laundry list of industries that they should, if you will, de-risk themselves from, the chilling effect on those industries is undeniable.

Mr. BACHUS. Thank you.

Mr. Jeffries, we are going to recognize you for 5 minutes now.

Mr. JEFFRIES. Mr. Chairman, I appreciate the——

Mr. BACHUS. Five or 6 minutes, as everybody else has had.

Mr. ISSA. I ask unanimous consent the gentleman have 7 or 8 minutes.

Mr. JEFFRIES. After that colloquy, I was going to suggest 10 or 15.

And I would just suggest that I find it ironic, there is a lot of concern about lawlessness in this town and in this institution. I would just think that regular order should prevail on this Subcommittee, particularly a Subcommittee where we have got a topic so inflammatory in terms of the subject matter, guilty until proven innocent.

And I guess I am struggling with that topic and reconciling its sort of explosive rhetoric with the notion that it seems that some Members have come into this Committee already presuming the guilt of the Justice Department and its activity connected with Operation Choke Point.

And I guess hypocrisy is not a constraint in this institution. I have figured that out over my 18 months. But nonetheless, hopefully we can have an exchange where I get some understanding as to the facts related to this program and not simply political rhetoric directed at the Department of Justice.

Now, it is my understanding that three separate decisions by courts in the Southern District of New York have upheld the Department of Justice's authority under FIRREA. Is that correct?

Mr. DELERY. Congressman, yes, those are referring to decisions that recognize the scope of the conduct that FIRREA prohibited in order to protect the integrity of the financial system.

Mr. JEFFRIES. And would it be fair to say that some District of New York courts are amongst the most commercially sophisticated district courts in the Nation, just given the nature of the subject matter that they often find before them?

Mr. DELERY. Yes, I think that that is fair. And I would also point out that these are the only three cases that I am aware of addressing the question. So all three courts to have addressed it have answered the question the same way.

Mr. JEFFRIES. Right. And these courts I believe also concluded that the phrase affecting a Federally insured financial institution includes financial institution that engages in fraudulent activity that harms itself. Is that correct?

Mr. DELERY. Yes.

Mr. JEFFRIES. Okay. And in *United States v. Countrywide*, I believe the court dismissed the defendant's argument that Congress did not intend FIRREA to include financial institutions that are parties to fraud and in fact characterized that position that seems to be supported by some members of this panel as utterly unconvincing. Is that correct?

Mr. DELERY. I don't remember the phrase specifically, but I do think all three decisions, looking at the text, structure, and legislative history of the statute, concluded that it provides broad antifraud protection where fraud affects a federally insured financial institution.

Mr. JEFFRIES. Okay. And I would just note for the record that we are preparing to sue the President based on alleged lawlessness, and some within the House of Representatives have concluded that the Article III court system should be the arbiter as to whether this President has engaged in "lawlessness." And that is fine. That is the prerogative of the majority in the House of Representatives.

But as it relates to this particular subject matter before us, as you have pointed out, every single court to look at the legality and the Justice Department's legitimacy to move forward as it has, has concluded that you are well within the boundaries of the law. And in fact, at least in one instance, has basically characterized the arguments being made by defendants and or their sympathizers as baseless in law.

And so there are a lot of things that we as a Committee and we as a Congress could be focused on. Certainly, I think the effort to hold financial institutions accountable for their actions and to make sure that consumers in the United States of America and those that we represent aren't harmed by reckless behavior, seems to be an appropriate thing for the Department of Justice to be engaging in, particularly given the fact that reckless behavior by financial institutions writ large caused the collapse of the economy in 2008, plunging us into the greatest economic crisis since the Great Depression.

And so I support the effort and applaud you, the Justice Department, for continuing to do what is necessary in the best interest of the American people. And I expect that as additional cases wind their way through the court system, they will equally be determined to be frivolous.

And I yield back.

Mr. BACHUS. I am sorry, you yield back?

Mr. JEFFRIES. Yield back, with 5 minutes to spare.

Mr. BACHUS. Okay, thank you. That was a shock to me. I wasn't expecting that. Thank you, Mr. Jeffries.

Mr. Holding?

Mr. HOLDING. Mr. Chairman, I have had my turn.

Mr. BACHUS. All right, thank you. I guess it is my turn.

Mr. Delery, in testimony on Tuesday you repeatedly stated that this is normal law enforcement initiative, and we are only interested in actual fraud. So you have issued 50 subpoenas. Is that correct?

Mr. DELERY. That is the ballpark for the number.

Mr. BACHUS. Okay. How many settlements have you procured?

Mr. DELERY. Again, as I indicated, so far there is one case that has been resolved; others are ongoing. And obviously some of those subpoenas——

Mr. BACHUS. When did you start issuing these subpoenas?

Mr. DELERY. It was in early 2013, so a little more than a year ago.

Mr. BACHUS. Eighteen months ago, 17 months ago, 16?

Mr. DELERY. Right.

Mr. BACHUS. And Four Oaks Bank is the only one that—so zero lawsuits or prosecutions, right?

Mr. DELERY. Again, there are ongoing both civil and criminal investigations.

Mr. BACHUS. Investigations, but no prosecutions.

Mr. DELERY. Not so far.

Mr. BACHUS. Okay. So you have issued 50 subpoenas.

Mr. DELERY. And again, some of the subpoenas related to the same matter.

Mr. BACHUS. To the same bank?

Mr. DELERY. Or to seeking information about the same—not necessarily to the same bank, but to related organizations or institutions that might have information——

Mr. BACHUS. But 50 different financial institutions received subpoenas?

Mr. DELERY. I am not sure that that is right. I think it is in the ballpark of 50 total.

Mr. BACHUS. The cases you cite, you talk about a 30 to 50 percent return rate or chargeback. That is pretty doggone high. I mean, that would alert anyone to something unusual going on. How did you come up with that 30 to 50 percent?

Mr. DELERY. So I referred to the merchants that are identified in the Four Oaks complaint. So there were more than a dozen merchants that Four Oaks knew about that had a return rate of over 30 percent. One was 70 percent?

Mr. BACHUS. Yeah, Wachovia, First Bank of Delaware, Four Oaks, I mean they all had return rates of 30 to 50 percent.

Mr. DELERY. Exactly, and Wachovia and First Bank of Delaware I think are also good examples, and the payment processor that was charged in connection with Wachovia, those are the prior cases that are——

Mr. BACHUS. Right. And you have highlighted that. I mean, Wachovia, First Bank of Delaware, all had these high return rates and chargebacks. And I am acknowledging that ought to be a red flag. But I notice your document request has a different return rate. It is 3 percent. It says that any customers' accounts that experience a return rate of 3 percent or greater in any 1-month period. So suppose you had someone that sold ammunition, magazine subscriptions, tobacco, firearms, coin shops, and they have had one check returned out of 25. That would put them under this category.

Why did you go from 30 to 50 percent to 3 percent? Three percent not over a year, but 3 percent in any 1-month period, which actually could be 3 checks within 1 month for somebody that did 100 checks. They could have three returned checks in a year fall under that.

Mr. DELERY. The 3 percent number comes from some of the information requests. That is not something that we viewed as a threshold for fraud and is not the basis for a charge.

Mr. BACHUS. But in your document request it says, number 6, on page 6.

Mr. DELERY. Right. In some of them we asked for information about returns over that number which was more than twice the average according to the industry groups. That was not intended to reflect——

Mr. BACHUS. And some industries are going to have a higher return rate. I mean, magazine subscriptions, there is nothing necessarily fraudulent about that.

I guess what I am saying, you are asking financial institutions to go through and find out any customer they had that had 3 percent of their checks return in 1 month that did any of these "high-risk" businesses.

Mr. DELERY. I think that in connection with requests that we make, we often have a discussion about the scope and what information they can provide in the way that a recipient——

Mr. BACHUS. Well, but you asked all of them that. Then they have to hire lawyers. Then they have to have these discussions with you? And a small payday lender or ammunition seller or somebody selling tobacco, I mean, they have got to hire a lawyer, they have got to come to you, they have got to come to you and say, hey, can we? Do you ever modify that 3 percent?

Mr. DELERY. My understanding is that there were discussions with some of the recipients about the scope and, again, what information they had that could be provided and what would be appropriate. So, again, that is a standard approach in——

Mr. BACHUS. But in fact in 4 it says, documents sufficient to identify payment processors or merchants or clients that experienced a return rate of 3 percent or greater in any 1-month period. Don't you think that is pretty low? That is a pretty wide net. I mean, that is a pretty wide net, isn't it?

Mr. DELERY. Again, that was a request for information that was set at a level that was double the industry average, as I understand it.

Mr. BACHUS. But in all your testimony you have highlighted companies that had—3 percent is not evidence of fraud, is it?

Mr. DELERY. I agree with that.

Mr. BACHUS. Okay.

Mr. DELERY. And we have not viewed it as that.

Mr. BACHUS. Right.

Mr. DELERY. I thinkit was an effort to find information.

Mr. BACHUS. But you are going down to 3 percent, but you admit that 3 percent in 1 month is not evidence of fraud.

Mr. DELERY. Not that amount per se. We don't have a absolute threshold for that.

Mr. BACHUS. Okay. Thank you. Well, it is an absolute—I mean, it is in your subpoenas, it is 3 percent.

Mr. DELERY. As a request for information, that is correct.

Mr. BACHUS. Well, it is a subpoena, it is a subpoena, it is a legal document that the bank has to go out and find all these people. You agree that banks like to avoid risk, right?

Mr. DELERY. I mean, that would be my understanding.

Mr. BACHUS. And they avoid it by de-risking. And in this case I am not saying you purposefully, personally wanted to have these banks jettison these clients, but they are going to avoid risk. You send them something, you attach a list of different businesses.

And it is also interesting that this list from the—I apologize. That is Rachel at Card Services. I would love for you all to go after them.

The ones that you highlighted actually in this thing you attached, and this was a document I guess you all prepared because you refer to the FDIC, you just talk about examples. And you use tobacco sales, pharmaceutical sales, payday and subprime loans, pornography, magazine subscriptions.

But, General, some that you didn't include were escort services or drug paraphernalia, which was on the original list. So kind of interesting that Ponzi schemes, pornography, you didn't include those, you included firearm sales, ammunition sales. Kind of interesting. How did you highlight that over pyramid schemes, pornography, or escort services?

Mr. DELERY. So, Congressman, these materials were prepared by the FDIC for their own regulatory purposes. And to my knowledge, the Department of Justice did not participate in choosing the examples.

Mr. BACHUS. When you attach this to your subpoena don't you realize that sends a message?

Mr. DELERY. Well, I think that it is important, if I could, to clarify again, that doing business with any particular industry, whether on a high-risk list of a regulator or not, was not the basis for receiving any of the subpoenas. We selected the recipients of the subpoenas because we had reason to believe that the recipients had evidence of fraud that was being conducted by either a financial institution or somebody else against a consumer. And the sources of information were prior investigations into fraudulent merchants or cooperating witnesses.

Mr. BACHUS. Yeah, I think when you issue a subpoena to a bank and you say, we are looking for fraud, and you say, ammunition sales, firearm sales, payday lending, you have to acknowledge that many banks said they have cut these folks loose. Tobacco sales.

Mr. DELERY. Congressman, I think it is also important to note that we have, in response to questions, taken a number of steps to make clear to the industry and to the public what we are and are not doing. And so, going back to last year, we have met with industry groups, we have communicated with them, we have written to Members of Congress to make clear that doing business with any particular industry we don't view as evidence of fraud.

And so I do think we take seriously the questions of effects on other institutions and have therefore been working publicly and with industry to explain what we are and are not doing To avoid that kind of result.

Mr. BACHUS. My Democratic colleagues have said they want to wrap this up. So let me just simply say to you that this is having the effect of shutting down these companies, whether that was intended or not. So thank you.

Mr. JOHNSON. Mr. Chairman?

Mr. BACHUS. Oh, you have another question. Sure.

Mr. JOHNSON. I would ask you to yield to me for a couple of questions.

Mr. BACHUS. Sure. I am sorry, two questions, or however many questions.

Mr. JOHNSON. The National Automated Clearing House Network Association, which governs the ACH Network through its self-regulatory operating rules, has repeatedly referred to banks as the gatekeepers of the ACH Network. Do you agree with that characterization of banks? Yes or no?

Mr. DELERY. I certainly agree that merchants need access to the banking system through a financial institution, if that is what that means. I am not familiar with that.

Mr. JOHNSON. And the ACH Network connects more than 12,000 financial institutions while over $40 trillion in value is supported annually through the ACH Network representing more than 22 billion transactions. And the average rate of returns or chargebacks is less than 1.5 percent on the ACH Network. Please discuss

whether higher return rates trigger certain diligence requirements for banks and payment processors.

Mr. DELERY. Well, certainly, Congressman, I think that among the evidence that we look to in evaluating fraud, particularly high return rates would be in that category as reflected in the Four Oaks case. Again, our cases are based on situations not just where a financial institution unwittingly processes a fraudulent transaction, but where they knowingly allow fraudulent merchants to access the payment system through their institution or deliberately look the other way against evidence of fraud, for example, by having a control in place and then turning it off to avoid seeing the answer. And a high return rate could be and has been, for example, in the Four Oaks case, evidence of repeated fraudulent withdrawals by consumers.

And I do think it is important to remember that at bottom these cases are about fraud against consumers. They started by noting the endless variety of fraud, different types of scams that consumers face all across the country, and by following where the money went from those scams to particular banks and payment processors that are not following the rules.

Mr. JOHNSON. And an indication that the rules are not being following is a high rate of return. And the industry standard is about 1.5 percent. Isn't that correct?

Mr. DELERY. Yes, that is my understanding.

Mr. JOHNSON. And the subpoena that my friends from the other side keep referring to puts the institution to which the subpoena was directed on notice that a 3 percent return rate is something that they should pay attention to.

Mr. DELERY. I guess the way I would say it, Congressman, is that some of the subpoenas asked for return rates over 3 percent, that that would be twice the ordinary average. Again, we did not view and do not view that level as evidence of fraud. The type of return rates we are talking about in Four Oaks, 30-plus, up to 70 percent, would be evidence of fraud.

Mr. JOHNSON. A 70 percent return rate would certainly authorize a civil action against that particular institution.

And with that I will——

Mr. BACHUS. And you have no debate for anyone on that.

And let me close by saying, the Democratic Senator from Hawaii, 11 members of Financial Services, Democrats, have written expressing their concerns over legitimate businesses being shut down.

And I will close by just, I want to read this to you, just to say go back, consider this. Powder Horn Outfitters sells shooting, archery, and fishing equipment in Hyannis, Massachusetts. It was recently turned down for a loan by its longtime bank. Powder Horn's owner says this. He cites Operation Choke Point. "Our loan was turned down not because of our credit. We had perfect financials and had been working with the same manager for 20 years. It was just because question sell guns, and they said that to us specifically, you sell guns." So it is having that effect.

Mr. DELERY. And, Mr. Chairman, hopefully this hearing, among other things, helps to explain our position that that is not the basis of the actions that we are bringing. We will continue our efforts to make clear what our policy is, which is to pursue fraud.

Mr. BACHUS. Hopefully you will take some of our concerns, like this 3 percent and others, into consideration, because I know that a lot of companies that are losing their bankers. Three percent in 1 month. And you said and I have said that in certain industries 3 percent is not that unusual. There are industries that deal with certain demographics, the average is 1.5, there are going to be stores in certain areas that are going to have 3, 4 percent, particularly in 1 month.

Consumer fraud is real. Go after that, not after an archery store. Thank you.

Mr. DELERY. Thank you.

Mr. BACHUS. And you are dismissed. And we appreciate your testimony and your candor.

Mr. BACHUS. Good morning. So this is our second panel, and we have an esteemed group of witnesses, starting out with Professor Levitin, Adam J. Levitin, Georgetown University Law Center.

Professor Levitin is a professor at Georgetown University. That pretty much goes without saying, doesn't it? But he specializes in bankruptcy, commercial law, and financial regulation. His research focuses on consumer and housing finance payments and debt restructuring.

He currently serves on the Consumer Financial Protection Bureau's Consumer Advisory Board, and he has previously served as the Bruce W. Nichols Visiting Professor of Law at Harvard Law School, and the Robert Zinman Scholar in Residence at the American Bankruptcy Institute, and the Special Counsel to the Congressional Oversight Panel for the Troubled Asset Relief Program.

Prior to joining the Georgetown faculty, Professor Levitin practiced in the Business Finance and Restructuring Department of Weil—is that Gotshal?

Mr. LEVITIN. Weil, Gotshal. But if you would like to curtail the biography. There is no reason everyone here needs to hear it.

Mr. BACHUS. Okay. And Weil, Gotshal & Manges?

Mr. LEVITIN. That is right.

Mr. BACHUS. LLP. And served as law clerk to the Honorable Jane R. Roth on the United States Court of Appeals for the Third District.

Professor Levitin received his JD from Harvard Law School, a masters in—is that philosophy?

Mr. LEVITIN. It is actually an M.Phil in history.

Mr. BACHUS. Okay.

Mr. LEVITIN. You are going to make my mom very proud.

Mr. BACHUS. And an AM from Columbia University, and an AB from Harvard College. His scholarship had won several awards, including the American Law Institute's Young Scholar's Medal.

We welcome you.

Mr. Scott Talbott, senior vice president of government affairs at the Electronic Transactions Association. He is responsible for developing and executing ETA's Federal and State legislative and regulatory strategies on behalf of ETA's more than 500 member companies.

Prior to joining ETA, Mr. Talbott served senior vice president for public policy at the Financial Services Roundtable where he directed the overall policy strategy, managed the daily legislative and

regulatory advocacy efforts, and directed communications. Mr. Talbott also served as counsel to the organization and managed the Roundtable's political action committee.

He has received numerous accolades in his tenure, including being named the top lobbyist by the Hill in both 2009 and 2011, as well as a winner for his work during the economic collapse of 2008 by the Washingtonian magazine.

In 2010 he appeared in the Oscar winning film "Inside Job." So you are a movie star, right? How about that. I didn't know that, Scott. Once named NPR's favorite bank lobbyist. He is a frequent contributor to both national and international media.

He joined the Roundtable in 1994 after working in the tax department's of Arthur Anderson and Ernst & Young. He received his BA from Georgetown University cum laude and his JD from George Mason University School of Law. So we have two Georgetown professors and a student.

Mr. David H. Thompson, managing partner, Cooper & Kirk. Mr. Thompson is a managing partner at that firm and joined the firm at its founding. Mr. Thompson has extensive trial and appellate experience in a wide range of matters. In commercial matters Mr. Thompson has had significant trial experience in litigating large claims for plaintiffs and defendants.

Serving as the de facto general counsel to several private companies, Mr. Thompson has developed significant practical business experience. Mr. Thompson has taken hundreds of depositions of senior executives, expert witnesses, high-ranking government and university officials, employees, and union leaders.

So you know how much subpoenas can cost, right?

Mr. THOMPSON. Yes, sir.

Mr. BACHUS. Thank you.

Mr. Thompson also has extensive experience in constitutional litigation. Mr. Thompson has litigated numerous cases involving freedom of speech, civil rights, voting rights, taking of property, Second Amendment and separation of powers issues.

Ah, Mr. Thompson also served as an adjunct faculty member at Georgetown University Law Center and a visiting professor at the University of Georgetown Law School, D.C. campus.

Mr. Thompson received his AB degree magna cum laude from Harvard University and received his JD degree cum laude from Harvard Law School.

All right, we finally have a witness that doesn't have a Georgetown, Harvard background here.

Our last witness is Mr. Peter G. Weinstock?

Mr. WEINSTOCK. Weinstock, yes, sir.

Mr. BACHUS. Weinstock. A partner at Hunton & Williams LLP. His practice focuses on corporate and regulatory representation of small to large regional and national financial institution franchises.

During the past several years Peter has devoted substantial time to regulatory law enforcement and internal investigations of financial institutions. He is co-practice group leader of the Financial Institutions Section. He has counseled institutions on more than 150 M&A transactions, as well as provided representation on security offerings and capital planning.

Mr. Weinstock has authored numerous articles in bank publications. His article "Acquisitions of Failed Banks Present Risk and Opportunity" was honored by the RMA Journal in 2011. He has spoken at over 150 banking conferences and seminars and is recognized at a top speaker and writer in his field.

He received his BA from State University of New York and his J.D. From Duke University School of Law. He is a member of the Texas Bar.

Mr. WEINSTOCK. Better basketball, Mr. Chairman, than Georgetown University.

Mr. BACHUS. You did what?

Mr. LEVITIN. Object.

Mr. WEINSTOCK. Better basketball than Georgetown University.

Mr. BACHUS. At Duke. That is right. Georgetown is kind of a whipping boy for Duke. Recently. All right.

Each of our witnesses' written statements will be entered into the record in its entirety.

And I am not going to ask you to restrict it just to 5 minutes. So if you want to take a little longer, don't feel rushed. But, anyway, you will see a light will turn red and kind of begin to wrap it up then.

All right. At this time Mr.—Professor Levitin, we will start with you.

TESTIMONY OF ADAM J. LEVITIN, PROFESSOR OF LAW, GEORGETOWN UNIVERSITY LAW CENTER

Mr. LEVITIN. Good morning, Mr. Chairman Bachus, Ranking Member Johnson, and Members of the Subcommittee. Thank you for inviting me to testify today.

Criticism of Operation Choke Point reflect a lack of understanding of payment systems, in general, and the Automated Clearing House, or ACH, payment system in particular.

Critics of Operation Choke Point claim that the Department of Justice has overstepped its legal authority under FIRREA, which is predicated on crimes that affect Federally insured financial institutions.

Operation Choke Point's critics claim that consumer frauds do not affect financial institutions. They are wrong. When a bank transmits a payment request in the ACH system, the bank warrants that the request was authorized by the consumer and that the requester complies with the laws of the United States.

This means that banks are vouching for the legitimacy of the payments in the ACH system. When payments turn out to be unauthorized or illegal, banks have liability. A similar situation exists for credit and debit card payments where banks are on the hook for chargebacks that merchants are unable or unwilling to pay.

Consumer fraud very much affects Federally insured financial institutions. Accordingly, Operation Choke Point is squarely within the Department of Justice's statutory authority under FIRREA.

Now, you may hear that the Department of Justice is abusing the concept of reputational risk. But I would note that there is a single mention of reputational risk in the only complaint filed in Operation Choke Point, that—the complaint against Four Oaks Bank.

Whatever issues there are with the concept of reputational risk, they do not at this point appear to be part of Operation Choke Point, and I think we should be very careful not to conflate the Department of Justice's civil investigation of specific fraud with other regulatory activity by prudential regulators. I think it is important that we keep them separate.

Critics of Operation Choke Point have also argued that the Department of Justice is trying to shut down legitimate, but disfavored, industries. This concern is unfounded.

Operation Choke Point focuses on banks that choose to process transactions that they know are fraudulent or that willfully ignore clear evidence of fraud. Operation Choke Point is about ensuring the banks comply with their anti-money laundering operations.

The basis for the Department of Justice's suit against Four Oaks Bank was that Four Oaks did not have reasonable controls in place and ignored the presence of really glaring red flags indicating illegal activity.

That said, there are objective measures of industries with higher consumer fraud rates, namely, the rate of ACH transactions that are returned as unauthorized. When dealing with these industries, banks cannot be lax in anti-money laundering compliance, and they may need to conduct further diligence.

Now, this does not mean that banks need to look through every image on a customer's porn Web site to see if there is child pornography or examine every payday loan for a Military Lending Act violation or ensure that every firearm sold by a customer is not sold to a convicted felon.

But banks do need to take reasonable steps to determine that their customer is doing a legitimate business and these are legitimate industries, but banks have to verify what the business actually is and not to ignore red flags like high unauthorized transaction return rates, high volumes of consumer complaints, or false representations of U.S. domiciles, was the case in Four Oaks Bank.

This is not making the banks cops. Instead, it is just emphasizing that banks cannot willfully turn a blind eye to illegal activity.

Concerns about spillover effects are also overstated. There are anecdotes, but no verified evidence of Operation Choke Point affecting legitimate businesses. There are no verified cases of banks terminating customer accounts because of Operation Choke Point.

Payday lenders have been having problems with bank account terminations for over a decade. In 2006, payday lenders testified about this to Congress. This is a problem that predates Operation Choke Point.

But even if Operation Choke Point were resulting in account terminations, it is not clear why this would be a problem, per se. Compliance with anti-money laundering regulations has costs, and that is especially true in dealing with high-risk businesses. Some banks may very well rationally decide that it isn't worthwhile to serve these businesses.

For other banks, however, Operation Choke Point is a business opportunity. Some of our nearly 7,000 banks will serve these high-risk businesses, but they will do so at a higher price, and this is just the free market at work.

In other words, Operation Choke Point might result in higher costs of banking services for higher risk merchants. There is nothing wrong with that. Banks should be pricing for risk, and high-risk merchants should have to pay their own freight.

The thing is high-risk merchants don't want to pay higher costs. They would rather be subsidized by getting a pass from anti-money laundering laws. And that is what they are here asking you for.

There is no reason that we should be subsidizing high-risk businesses like escort services, payday lenders, pornographers, or purveyors of racist material. Yet, pressuring the Department of Justice to back off Operation Choke Point is an attempt to subsidize these high-risk businesses, and it is an attempt to do so that comes at the expense of homeland security. Congress shouldn't be doing that.

Operation Choke Point is a legitimate exercise of the Department of Justice's authority under FIRREA to investigate and prosecute frauds affecting Federally insured financial institutions. Banks need to take their anti-money laundering responsibilities seriously. Operation Choke Point should be applauded, not criticized.

Thank you.

[The prepared statement of Mr. Levitin follows:]

GEORGETOWN UNIVERSITY LAW CENTER

Adam J. Levitin
Professor of Law

Written Testimony of

Adam J. Levitin
Professor of Law
Georgetown University Law Center

Before the United States House of Representatives
Judiciary Committee
Subcommittee on Regulatory Reform, Commercial, and Antitrust Law

"Guilty Until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's *Operation Choke Point*"

July 17, 2014
9:30 am

Witness Background Statement

Adam J. Levitin is a Professor of Law at the Georgetown University Law Center, in Washington, D.C., where he teaches courses in financial regulation, structured finance, contracts, bankruptcy, and commercial law. He is also the lead author of the chapter on Electronic Funds Transfers in the National Consumer Law Center's treatise on *Consumer Banking and Payments Law* (5th ed. 2013).

Professor Levitin has previously served as the Bruce W. Nichols Visiting Professor of Law at Harvard Law School, as the Robert Zinman Scholar in Residence at the American Bankruptcy Institute, and as Special Counsel to the Congressional Oversight Panel supervising the Troubled Asset Relief Program (TARP). Professor Levitin currently serves on Consumer Financial Protection Bureau's Consumer Advisory Board.

Before joining the Georgetown faculty, Professor Levitin practiced in the Business Finance & Restructuring Department of Weil, Gotshal & Manges, LLP in New York, and served as law clerk to the Honorable Jane R. Roth on the United States Court of Appeals for the Third Circuit.

Professor Levitin holds a J.D. from Harvard Law School, an M.Phil and an A.M. from Columbia University, and an A.B. from Harvard College. In 2013 he was awarded the American Law Institute's Young Scholar's Medal.

Professor Levitin has not received any Federal grants or any compensation in connection with his testimony, and he is not testifying on behalf of any organization. The views expressed in his testimony are solely his own.

© 2014, Adam J. Levitin

Mr. Chairman Bachus, Ranking Member Johnson, Members of the Subcommittee:

Good morning. Thank you for inviting me to testify at this hearing. My name is Adam Levitin. I am a Professor of Law at the Georgetown University, where I teach courses in financial regulation and structured finance, among other topics. I also serve on the Consumer Financial Protection Bureau's statutory Consumer Advisory Board. Among other publications, I am a co-author of the National Consumer Law Center's treatise of *Consumer Banking and Payments Law* (5th ed. 2013), and am the primary author of that treatise's materials on Automated Clearing House (ACH) transactions. I am here today as one of the few academics in the United States who writes and teaches about the ACH system; I am not testifying on behalf of the CFPB or its Consumer Advisory Board.

The fuss over the Department of Justice's *Operation Choke Point* reflects a fundamental lack of understanding of the operation of payment systems. *Operation Choke Point* aims to reduce consumer fraud by ensuring that banks that provide payment intermediary services comply with their existing legal obligations under the Bank Secrecy Act and Anti-Money Laundering regulations. Critics of *Operation Choke Point* argue that the Department of Justice is overreaching it is use of the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA) because the consumer frauds targeted by *Operation Choke Point* do not "affect" financial institutions as required by FIRREA.

Critics of *Operation Choke Point* fail to recognize, however, that the banks in the ACH system warrant the authorization and lawfulness of the transactions they initiate. This means that the banks assume liability themselves when handling fraudulent requests for payment. Moreover, banks' that fail to adequately supervise their customers risk expulsion from the ACH system under that system's private rules; few banks can operate competitively without access to the ACH system. Accordingly, use of the ACH system for consumer fraud very much "affects" banks. Banks' direct financial exposure means that the Department of Justice is squarely within its grant of authority when bringing prosecutions under FIRREA.

It is not a new idea that banks need to have adequate controls and risk management, particularly in regard to the oversight of third-party payment processors that serve as agents for ACH payees. Prudential bank regulators have for years emphasized the need for such oversight in regulatory guidance,[1] as has the private bank membership organization that sets the rules for the ACH system.[2] Third-party payment processors raise particular money laundering and payment warranty risks for banks when banks do not know the customers of the third-party payment processors and cannot verify that the customers are engaged solely in legitimate business. Indeed, bank regulators have repeatedly brought enforcement actions when banks have failed to adequately

[1] *See, e.g.*, FDIC, Managing Risks in Third-Party Payment Processor Relationships, Supervisory Insights, Summer 2011; OCC, Bulletin 2006-39, Automated Clearing House Activities, Sept. 1, 2006.

[2] NACHA, *Third-Party Sender Case Studies: ODFI Best Practices to Close the Gap*, An ACH Risk Management White Paper (2009).

© 2014, Adam J. Levitin

ensure the integrity of the payment system by failing to properly oversee third-party payment processors.[3]

When banks do not know their customers or, in the case of third-party payment processors (which are really pass-through entities), their customers' customers, there is an inherent risk of money laundering. *Operation Choke Point* is insisting that banks take their anti-money laundering responsibilities seriously. While *Operation Choke Point* is aimed at consumer fraud, the same controls necessary to ensure that the ACH system is not used to facilitate consumer fraud also ensure that it is not used to facilitate narcotics trafficking or financing for terrorism. The Department of Justice should be lauded, not lambasted, for its efforts to make sure that banks take their anti-money laundering responsibilities seriously.

If we want to ensure that our financial system is not used to facilitate evasion of US laws and terrorism financing, it is imperative that banks rigorously adhere to anti-money laundering rules, such as the "know your customer" requirement, and that anti-money laundering regulations not be undercut by use of third-party payment processors that mask the identity of the ultimate customer.

Attempts to hamper the Justice Department's enforcement of anti-money laundering laws are effectively a subsidy to high-risk businesses. When banks are not required to fulfill their anti-money laundering obligations, it enables risky merchants to avoid paying for the higher compliance costs they impose on banks. Congress should not be using its oversight power to subsidize high-risk businesses, such as payday lenders, on-line gun shops, escort services, on-line gambling parlors, purveyors of drug paraphernalia or racist materials, and pornographers, that serve no clear public purpose, much less at the expense of homeland security.

I. Understanding the ACH System

The automated clearing house or ACH is an electronic payment method for moving funds between accounts at depository institutions. ACH is one of the largest payment methods for business and consumer transactions. In 2013, there were nearly 22 billion ACH transactions for nearly $39 trillion performed in the United States.[4] Despite the volume of ACH payments, ACH remains one of the least familiar payment systems to consumers because it does not have a distinctive retail façade because ACH transactions do not require a special access device like a check or payment card. Instead, they merely require a transmission of a bank account and routing number, which can be done orally, in print, or electronically.

---

[3] *See, e.g.*, FDIC, Consent Order FDIC-10-845b, *In the Matter of SunFirst Bank, St. George, Utah*, Nov. 9, 2010; OCC, Consent Order, *In the Matter of: Wachovia Bank, Nat'l Ass'n, Charlotte, North Carolina*, AA-EC-10-17, Mar. 12, 2010 ($50 million civil monetary penalty; FinCEN, Assessment of Civil Monetary Penalty, *In the Matter of: Wachovia Bank, Nat'l Ass'n, Charlotte, North Carolina*, Number 2010-1, Mar. 12, 2010 ($110 million civil monetary penalty); U.S. v. Wachovia Bank, N.A., Deferred Prosecution Agreement, No. 10-20165-CR-LENARD (S.D. Fla., Mar. 16, 2010); U.S. v. First Bank of Delaware, No. 12-6500 (E.D. Pa.) ($15 million civil monetary penalty and surrender of bank charter); FDIC, Consent Order FDIC-12-367b, *In the Matter of Meridian Bank, Paoli, Pennsylvania*, Oct. 22, 2012.

[4] NACHA, ACH Network Statistics 2013.

© 2014, Adam J. Levitin

Different rules govern consumer and business ACH transactions. ACH transactions involving consumers are governed by a combination of the Electronic Funds Transfer Act and Regulation E thereunder and the rules of the National Automated Clearing House Association (NACHA), a not-for-profit membership association of banks that sets the standards for ACH operations in the United States.[5] Business-to-business ACH transactions are governed by NACHA rules and contract law; NACHA rules are somewhat different for business-to-business ACH transactions than for consumer transactions.

A. Parties to an ACH Transaction

Structurally, an ACH transaction looks much like debit card or credit card transaction. An ACH transaction involves (at least) five parties: an Originator, an Originator's depository financial institution (ODFI), an ACH Operator, a Receiver, and a Receiver's depository financial institution (RDFI). Sometimes there will also be a Third-Party Payment Processor (TPPP) involved as well, which serves as an agent for the Originator.

Both the ODFI and RDFI are always banks. The Originator (or TPPP, if one is involved in the transaction) has a bank account at the ODFI, while the Receiver has a bank account at the RDFI. The ODFI and RDFI each have accounts with the ACH Operator. There are only two ACH Operators in the United States: the Federal Reserve System's FedACH and the Clearing House's Electronic Payments Network.

B. How an ACH Transaction Works

In an ACH transaction, the Originator instructs the ODFI to submit a debit or credit instruction to the ACH Operator. The ACH Operator transmits the instruction to the RDFI, which will then credit or debit the Receiver's bank account. An ACH transaction can be either a credit or debit transaction, meaning that it can involve the Receiver's bank account being credited or debited. Irrespective of whether the Receiver's account is credited or debited, data flows are the same in all ACH transactions, and explain the ACH system's terminology: data flows always start with the Originator and end with the Receiver. In an ACH credit transaction, the data and funds move the same direction, from Originator to Receiver, while in an ACH debit transaction, the data flows from Originator to Receiver, but the funds flow the opposite direction. Because *Operation Choke Point* involves only ACH debit transactions, in which the Receiver's account is debited, I will focus on these transactions; somewhat different rules apply to ACH credit transactions, such as direct deposit.[6]

An ACH debit transaction involves an instruction to pull funds from a deposit account, whereas an ACH credit transaction involves an instruction to push funds from a deposit account. In an ACH debit transaction, the Originator (the payee) directs the ODFI to request that the RDFI transfer funds from the account of the Receiver (the payor) at the RDFI. In order to do so, the Receiver must have authorized the transaction. After obtaining the Receiver's authorization, the Originator transmits the transaction

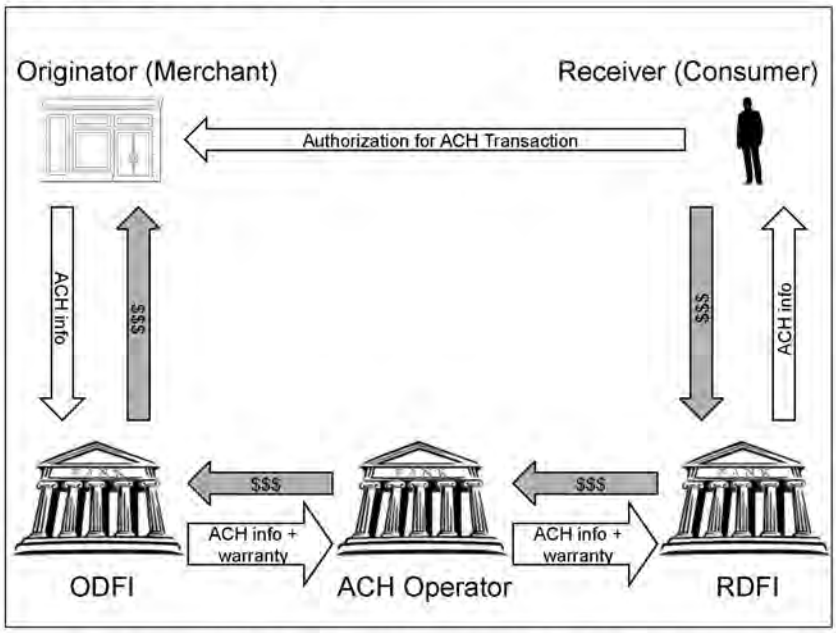
[5] NACHA Rules are a private set of industry self-regulatory rules, adopted by either a ¾ vote of NACHA members of a 2/3 weighted transaction volume vote of NACHA members. In other words, NACHA Rules are rules that banks themselves think are necessary.

[6] NACHA 2013 Operating Guide at OG2.

© 2014, Adam J. Levitin

information, including the Receiver's bank routing and account number to the ODFI. The ODFI then formats this information into an electronic file (an ACH file). The ODFI will then transmit the ACH file to the ACH Operator, which will transmit it to the RDFI, which will debit the account of the Receiver (i.e., the payor), transmit the funds to the ACH Operator, which will credit the ODFI's account, with the ODFI then settling the funds into the Originator's account at the ODFI.[7] Figure 1, below, illustrates an ACH debit transaction.

Figure 1. ACH Debit Transaction



To illustrate, consider an ACH debit transaction to collect a payday loan. In this transaction, the payday lender is the Originator, and the consumer is the Receiver. The payday lender's bank is the ODFI, and the consumer's bank is the RDFI. If the payday lender has received authorization for an ACH debit from the consumer, the payday lender may instruct its bank (the ODFI) to transmit an ACH debit item to the consumer's bank (the RDFI) through the ACH Operator. If there is money in the consumer's account, the

[7] ACH is a batch processing system, which means that individual transactions are not processed in real time. Instead, the ODFI accumulates ACH transactions and sorts them by destination for electronic transmission to the ACH Operator at a predetermined time. NACHA Operating Guide 2013, at OG1. The transactions batched in a particular time period are netted out by the ACH Operator among the various ODFIs and RDFIs in the system. The batch processing creates economies of scale as compared to the alternative of real time gross settlement such as is used in FedWire wire transfers (the continuous settlement of individual funds transfers on an order by order basis without netting).

© 2014, Adam J. Levitin

consumer's bank will debit the account and transfer the funds to the payday lender's bank through the ACH Operator.

C. ACH Returns

If there is no money in the consumer's account, the ACH debit item will be "returned." *An ACH "return" item is separate and distinct from a return of merchandise paid for via ACH.* Thus, a firm like Zappos, which sells shoes and other merchandise on-line, has a high rate of returns, but this does not mean that Zappos has a high ACH return rate. If a customer pays for shoes from Zappos via ACH and then returns shoes to Zappos, there is not normally an ACH return. Instead, Zappos would return the funds via an offsetting ACH credit.

Similarly, if it turns out that the consumer did not authorize the ACH debit and promptly notifies its bank after the funds have been debited, then the consumer's bank will "return" the ACH debit item and look to be reimbursed by the payday lender's bank for the funds that were improperly debited from the consumer' bank account. The consumer's bank will have a right to the funds from the payday lender's bank because the payday lender's bank has warranted that the transaction was authorized, that the transaction complies with NACHA Rules, including that the ACH entries do not "violate the laws of the United States," and indemnified the consumer's bank for any costs arising from an unauthorized transaction.[8] The payday lender's bank will be on the hook for these funds; it will have the right to recover them from the payday lender, but if the payday lender is out of business or insolvent, the payday lender's bank will bear the loss. The important point to see here is that the payday lender's bank is vouching for the transaction and may be liable for it.

D. Third-Party Payment Processors

Some ACH transactions involve a Third-Party Payment Processor (TPPP). A TPPP serves as an agent for the Originator. The Originator will transmit the transaction information to the TPPP, which will in turn transmit the information to the ODFI. In some cases, TPPP are allowed to have direct access to the ACH Operator for debit transactions.[9] Figure 2, below, illustrates an ACH debit transaction involving a TPPP.

There are legitimate uses of TPPP, which have specialization and technical capacities many Originators lack. The use of TPPPs began in the context of payroll management firms that were making ACH *credit* transactions (direct deposit), where funds were being transferred *to* consumers' accounts. ACH debit involves transfers *from* consumers' accounts and raises concerns about whether the transactions are authorized.

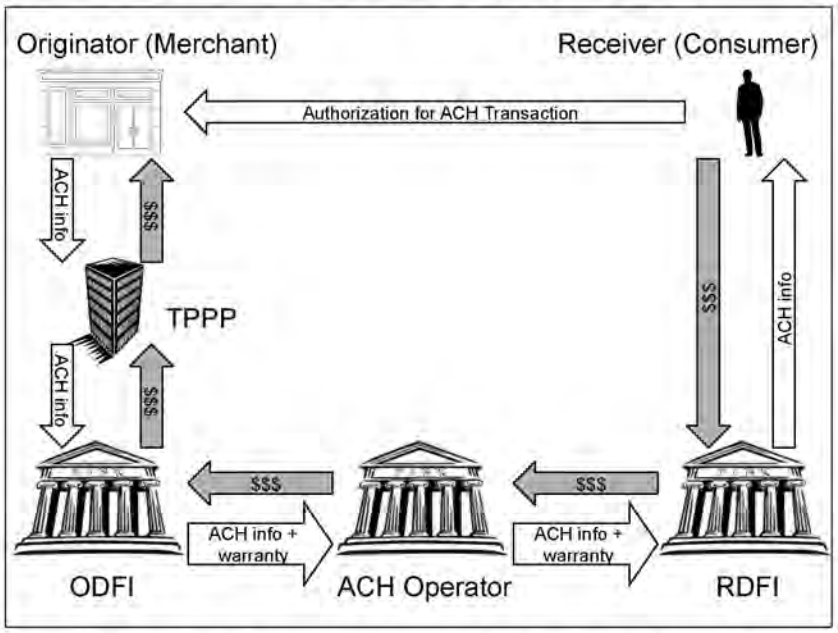
NACHA Rules aim to ensure the integrity of the ACH payment system and the trust and confidence of its users. Accordingly, NACHA Rules require ODFIs to monitor Originators' or TPPP's return rates for unauthorized transactions. NACHA Rules currently have a 1% threshold for unauthorized transaction return rates; a pending proposal would lower the threshold to 0.5%.[10]

---

[8] NACHA Rules 2.4.1 (ODFI warranties to RDFI); 2.4.4 (ODFI indemnification of RDFI).
[9] NACHA Rule 8.2.2.8.
[10] NACHA Rules 2.17.2.1, 10.2.1.

© 2014, Adam J. Levitin

Figure 2. ACH Debit Transaction with Third-Party Payment Processor



If an unauthorized transaction return rate exceeds 1%, then within 10 banking days the ODFI must submit to NACHA various information about the Originator or TPPP submit a plan for reducing the return rate to no more than 1% within thirty days and must in fact achieve such a reduction and maintain it for an additional 180 days.[11] If the ODFI fails to do so, it is subject to fines or suspension by NACHA.[12] NACHA fines and NACHA suspension, in particular, present a material risk for ODFIs. As a result, ODFIs will often simply terminate their business relationship with Originators whose unauthorized transaction return rates exceed the 1% threshold.

Because Originators with high unauthorized return rates risk being cut out of the ACH system, they often seek to use TPPPs to mask their return rates. TPPP typically serve multiple Originators. Because the return rate for a TPPP with multiple Originators is the transaction weighted average return rate of all of its Originators, an Originator that uses a TPPP can have an unauthorized transaction return rate that exceeds the NACHA threshold if the TPPP also serves Originators with low return rates. Thus, the use of TPPPs enables Originators with high unauthorized transaction return rates to maintain access to the ACH system. NACHA has recognized this risk and since July 18, 2010 has

[11] NACHA Rules 2.17.2.1; 2.17.2.2.
[12] NACHA Rules 10.2.2.

© 2014, Adam J. Levitin

required that ODFI's contracts with TPPPs include provisions that give the ODFI the right to terminate or suspect the contract or to terminate or suspend any Originator of the TPPP.

II. The Department of Justice's FIRREA Authority

Section 951(g) of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA) authorizes the Department of Justice to issue subpoenas to investigate potential wire fraud "affecting a federally insured financial institution".[13] This is exactly what the Department of Justice has done as part of *Operation Choke Point*.

As the controversy over Operation Choke Point appears to be centered on whether illegal or unauthorized ACH transactions are "affecting a federally insured financial institution" rather than on whether the predicate elements of wire fraud exist, my testimony is limited to the "affecting a federally insured financial institution" issue. As a starting matter, case law is clear that a bank is affected when there is merely "a new or increased risk of loss"; courts have uniformly held that an actual loss is not required by FIRREA.[14]

Critics of *Operation Choke Point* contend that payments on illegal or unauthorized underlying transactions affect only merchants and consumers, not financial institutions. They are wrong. Such a contention shows a fundamental lack of understanding of payment systems in general, and of the details of the ACH system in particular. Critics of *Operation Choke Point* simply do not understand how the ACH system operates and lack familiarity with the NACHA Rules that provide the legal framework for ACH transactions.

All non-real time payment systems involve credit risk for the banks that serve as intermediaries between payors and payees. If a transaction is reversed or refused, a bank can find itself a creditor of payor or payee, and if the payor or payee is insolvent, then the bank will take the loss. While the dollar amount for any single transaction may not be large, the cumulative exposures can be material.

ODFI banks in the ACH system expressly assume credit risk because they warrant the authorization and rules compliance of all ACH debit entries, including that the entry is not in violation of the laws of the United States. While the ODFI banks may be indemnified by or have upstream warranties from the TPPPs or Originators, these indemnities and warranties are only as good as the credit of the TPPP or Originator. In other words, ODFIs are assuming credit risk on illegal or unauthorized ACH transactions. Thus, illegal or unauthorized ACH transactions are plainly "affecting a federally insured financial institution". Moreover, ODFIs that serve Originators or TPPPs with excessive

---

[13] 12 U.S.C. § 1833a(a), (c), (g); 18 U.S.C. § 1343 (wire fraud).

[14] *See, e.g.*, *United States v. Serpico*, 320 F.3d 691 (7th Cir. 2003); *United States v. Mullins*, 613 F.3d 1273 (10th Cir. 2010); *United States v. Ghavami*, 2012 U.S. Dist. LEXIS 97931 (S.D.N.Y. July 13, 2012); Bank of N.Y. Mellon, 941 F. Supp. 2d 438 (S.D.N.Y. 2013); *United States v. Wells Fargo Bank, N.A.*, 972 F. Supp. 2d 593 (S.D.N.Y. 2013); *United States v. Countrywide Fin. Corp.*, 2014 U.S. Dist. LEXIS 19985 (S.D.N.Y. Feb. 17, 2014).

© 2014, Adam J. Levitin

unauthorized transaction returns risk being fined or suspended by NACHA, which would mean being cut out of the ACH system and unable to send or receive ACH items. Again, illegal or unauthorized ACH transactions are plainly "affecting a federally insured financial institution".

Thus, to the extent that an underlying consumer fraud utilizes ACH system, it is using a wire communication as part of a scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses with the intent to defraud. When an ODFI bank knowingly participates in such a scheme, it too is engaged in a wire fraud. The use of the ACH system to facilitate wire fraud necessarily "affects" the ODFI banks used by the fraudsters because the ODFI banks warrant the authorization and lawfulness of the transactions in the ACH system. This means that the fraudsters' ODFI banks are themselves potentially on the hook for the transactions. Moreover, ODFI banks that fail to adequately supervise their customers may be suspended from the ACH system. Because such consumer frauds to "affect" banks by posing real and material financial risk to them, it is appropriate for the Department of Justice to bring enforcement actions under FIRREA.

III. Account Terminations as a Result of *Operation Choke Point*

The Department of Justice's investigation into the use of the ACH payment system to facilitate consumer fraud has unquestionably encouraged banks to reexamine their Bank Secrecy Act/Anti-Money Laundering compliance, as well as their NACHA Rules compliance. In some case this might have resulted in banks deciding it was more cost effective to terminate business relationships than to undertake the necessary steps to ensure that the relationship was in compliance with the necessary legal requirements. It bears emphasis, however, that there are no verified cases of banks terminating accounts in direct reaction to *Operation Choke Point*; merely because an account was terminated after the commencement of *Operation Choke Point* does not mean that there was a causal connection, even if the account holder was in a "high risk" business.[14] Indeed, high-risk merchants have been having their accounts terminated since well before *Operation Choke Point.*

Even if banks have been terminating high-risk (but legal) accounts in response to *Operation Choke Point*, there is no reason for Congressional intervention. Such account terminations are nothing more than the normal operation of the free market. All markets are legally constituted and regulated. Legal compliance has costs; there is a cost to having anti-money laundering laws. Just as banks need to ensure that they are not providing payment services for drug dealers and terrorists, they also need to make sure that they are not providing payment services for child pornography transactions or for gun sales to convicted felons. If the cost of legal compliance is greater than the benefit to a bank from a customer relationship, the bank will rationally terminate the customer relationship.

Unless one believes that there is a serious market failure in the provision of business banking services, some of the nation's nearly 16,000 banks and credit unions

[14] *See*, Dana Liebelson, *Is Obama Really Forcing Banks to Close Porn Stars' Accounts? No, Says Chase Insider*, MOTHER JONES, May 8, 2014, *at* http://www.motherjones.com/politics/2014/05/operation-chokepoint-banks-porn-stars.

© 2014, Adam J. Levitin

will be willing to assume these high-risk businesses as customers…if these high-risk customers are willing to pay enough to cover banks' costs of servicing them in full legal compliance. Therefore, Congressional pressure on the Department of Justice to terminate *Operation Choke Point* is functionally providing a subsidy to high-risk businesses by allowing them to avoid the higher fees banks will charge in order to cover their additional costs of complying with anti-money laundering regulations for the high-risk businesses.

It bears emphasis that the account terminations are the result of banks making rational decisions about the costs of legal compliance; they are not at the directive of the Department of Justice. The Department of Justice's consent order with Four Oaks Bank does not prohibit Four Oaks Bank from dealing with payday lenders or from dealing with TPPPs that deal with payday lenders. Instead, it prohibits Four Oaks Bank from dealing with TPPPs that have in the past two years serviced payday lenders with high return rates for unauthorized transactions, data quality, or total returns. All the Department of Justice is doing is its job—enforcing FIRREA and the Bank Secrecy Act/Anti-Money Laundering regulations. Access to the financial system is a privilege, not a right, and it is given federal insurance of the financial system, it is reasonable to demand that banks that fail to institute proper risk management controls exclude high-risk customers from the system.

IV. The Supposedly Slippery Slope

Critics of *Operation Choke Point* have raised a straw man argument that *Operation Choke Point* is the first step in shutting down legitimate, but politically disfavored businesses: today the payday lenders, tomorrow the gun shops and pornographic websites, the next day the abortion clinics or the Tea Party….[15]

This slippery slope argument is flawed. The industries that have been flagged as high-risk merchant categories are so-flagged because of they have high unauthorized transaction rates, using objective metrics. While critics of *Operation Choke Point* claim that it is affecting legitimate coin dealers, on-line gun shops, and pornographers, these critics ignore the undisputed fact that coin dealers, on-line gun shops, and pornography websites have high unauthorized transaction rates.[16]

The categorization of merchant groups such as coin dealers, on-line gun shops, on-line gambling, escort services, purveyors of drug paraphernalia or racist materials, and pornographers as high-risk is not simply a matter of regulatory fiat. Instead, it is reflected in the price terms that the free market sets. Banks already charge these merchants much higher fees for banking services precisely because of the risks they pose. For example, pornography websites might pay 15% of a transaction amount to their bank to accept a credit card payment because of a high percentage of their transactions are disputed: "I didn't subscribe to that smut! I'm a happily married man!" In contrast, a

[15] *See, e.g.*, Todd Zywicki, "Operation Choke Point," Volokh Conspiracy, May 24, 2014, *at* http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/24/operation-choke-point/. *See also*

[16] These businesses are often high risk because of consumer fraud, rather than merchant fraud, but both can exist. These businesses may be high risk because of consumer fraud because consumers will "pay" for the transaction and obtain the merchandise, but then dispute that the transaction was authorized. In other words, consumers' fraud on merchants, as well as merchants' frauds on consumers may be responsible for high unauthorized transaction rates.

© 2014, Adam J. Levitin

low-risk business such as Wal-Mart might pay around 1%-2% of a credit card transaction.

If abortion clinics and the Tea Party—or any other party initiating ACH debit transactions—have high unauthorized transaction rates, it would be legitimate for regulators to pay more attention to TPPPs that service them and to insist that banks verify their identity and the legitimacy of their businesses. NACHA's 1% unauthorized transaction return threshold—a threshold set by a supermajority vote of NACHA's bank members and not by federal regulators—presents an objective measure of risk that is not susceptible to manipulation for political vendettas.

If and when federal regulators pressure banks to cease doing business with legitimate, *low-risk* businesses, there would be cause for concern. That has not happened yet. Instead, what has happened is that legitimate, but *high-risk* businesses have found themselves having to internalize the costs of their own risky business models because the Department of Justice has insisted that banks fulfill their obligations under the anti-money laundering regulations. Rather than paying their own freight, however, these high-risk businesses have run to Congress complaining about *Operation Choke Point* and asking Congress to use its oversight authority to get the Department of Justice to back off.

Make no mistake about it: these high-risk businesses are in effect seeking a subsidy from Congress by seeking to be effectively exempted from anti-money laundering laws. It is shocking that Congress would even humor such a request. Homeland security should not be compromised in order to subsidize high-risk businesses like payday lenders, escort services, on-line gun shops, on-line gambling parlors, purveyors of drug paraphernalia or racist materials, and pornographers.

V. Banks as "Policemen"

Some critics of *Operation Choke Point* have objected to banks being dragooned into the role of "policemen".[17] This objection is off base. *Operation Choke Point* does not force banks to be the "policemen" of the financial system. Instead, it insists that banks have in place reasonable controls and that they do not willfully ignore evidence of illegal transactions.

Banks are not like other businesses. They are public instrumentalities. Banks receive special (and limited) charters and federal insurance that shelter them from competition and subsidize their risk-taking. The deal for receiving these privileges is serving public purposes. Ultimately we do not ask a lot from banks: fair lending, community reinvestment, and anti-money laundering diligence.

Operation Choke Point is ultimately an anti-money laundering enforcement that requires that banks take their "Know Your Customer" duty seriously. Banks that deal with TPPPs must look through them to the ultimate Originator of an ACH transaction, just as they would be expected to look through an Originator's corporate shell to determine a client's real business. Ultimately, this is a matter of having reasonable processes, not perfect results. The basis for the Department of Justice's suit against with

[17] Frank Keating, *Justice Puts Banks in a Choke Hold*, WALL ST. J., April 24, 2014.

© 2014, Adam J. Levitin

Four Oaks Bank was that it did not have reasonable controls in place and ignored the presence of red flags indicating potential illegal activity.

Operation Choke Point does not demand that banks to evaluate every image on a pornography website for child pornography or every loan from a payday lender for violation of the Military Lending Act or state law. But banks do need to take reasonable steps to determine that the Originator is doing a legitimate business and not ignore red flags like high unauthorized transaction return rates or high volume of consumer complaints that mandate further diligence. This is not making the banks cops; instead, it is just emphasizing that banks cannot willfully turn a blind eye to illegal activity.

Conclusion

Operation Choke Point is a legitimate exercise of the Department of Justice's authority under FIRREA to investigate and prosecute wire frauds affecting federally insured financial institutions. Unauthorized ACH transactions, such as those in consumer frauds, pose direct financial risk to federally insured banks. The concerns that *Operation Choke Point* will be used to shut down legitimate businesses are unfounded. Instead, *Operation Choke Point* will ensure that banks take their anti-money laundering responsibilities seriously. *Operation Choke Point* should be applauded, not criticized.

When banks are required to fulfill their obligations under the anti-money laundering laws, high-risk industries that impose greater compliance costs on banks may find it costlier to obtain banking services. This is the cost of having anti-money laundering laws. There is no reason that Congress should subsidize high-risk businesses that serve no public purpose such as the purveyance of drug paraphernalia or racist materials, on-line gun shops, payday lenders, and pornographers, much less at the expense of homeland security. Surely homeland security should come before drugs, on-line gun purchases, racism, payday loans, and pornography.

© 2014, Adam J. Levitin

Mr. BACHUS. Thank you.
Mr. Talbott.

TESTIMONY OF SCOTT TALBOTT, SENIOR VICE PRESIDENT OF GOVERNMENT AFFAIRS, THE ELECTRONIC TRANSACTION ASSOCIATION

Mr. TALBOTT. Chairman Bachus, Ranking Member Johnson, Members of the Subcommittee, my name is Scott Talbott. I head up government affairs for the Electronic Transactions Association. ETA appreciates the opportunity to participate in the Subcommittee's hearing on the Operation Choke Point.

ETA is an international trade association representing companies primarily involved in all aspects of electronic payments. We focus on credit cards, debit cards, and prepaid cards. In 2013, we processed over 100 billion transactions for about $5 billion worth of goods and services. We are the choke in Choke Point.

In summary, the ETA strongly supports vigorous enforcement of existing laws and regulations to prevent fraud, but we believe that Operation Choke Point is the wrong execution of the right idea.

The payments industry has always been committed to fraud. It is part of what we do. And I am not here to defend fraudulent actors.

Consumers in the United States choose electronic payments over cash and checks because they have zero liability for fraud. And the cost of that fraud is generally borne by ETA members. So ETA members commit massive amounts of resources in time and money into detecting and eliminating fraud.

Every participant in the payment system has developed effective due diligence programs to both prevent fraudulent actors from accessing the payment system and to terminate access from fraud is determined. For example, last year, 5 percent of merchant applications were denied and ETA members terminated more than 10,000 fraudulent merchants.

As you know, fraud never stops. It never sleeps. And so the industry can—must continuously develop new techniques to fight it. With the expansion and ubiquitousness of the Internet, that creates new challenges. As we build a 10-foot wall, the crooks build an 11-foot ladder.

So, in response, ETA developed new guidelines that we have put out for the entire industry, not just ETA members, that represent 100 pages of due diligence designed to increase the underwriting methods and enhance the ability of the industry in this new day and age to detect and eliminate fraud.

These guidelines are drawn based on existing rules that exist both at individual companies and across the payments ecosystem, and they also draw from Operation Choke Point. It is part of the regulatory environment that we operate in. And so we have included many references and similar concepts in the guidelines.

Our concerns with Operation Choke Point are that it neglects the payments industry's efforts in this area to detect and eliminate fraud. It creates a confrontational approach that has a chilling effect on the payments industry's ability and willingness to report fraudulent merchants to law enforcement mainly because the pay-

ments industry believes that they may be subject to enforcement action if they do report.

And this harms three categories of merchants. One, we have seen evidence of companies dropping whole classes of merchants. We see increased costs for merchants, not just those in high-risk categories, but across the system. And we see—we could see a restriction of access to the payment system in the future for new merchants trying to gain it.

What our main particular focus is with Choke Point, what our main concern is, is that regulators and law enforcement agencies seem to be changing the long-standing policy of only focusing on those payment companies who have actively engaged in fraud.

It appears that OCP is—Operation Choke Point is trying to hold law-abiding payment companies liable for something as simple as a high return rate or simply providing merchants access to the payment system. If this is the case—and this is our fear, that the consequences I just mentioned will come to bear.

The Operation Choke Point is not just limited to—as everyone knows, to Department of Justice. Other regulators and law enforcement agencies appear to be getting into the game or adopting similar approaches. For example, ETA members have received communications from the FTC with Operation Choke Point-like questions involved.

We believe there are more targeted and more efficient ways to detect and eliminate fraud. The payments industry makes a better partner than a target in this effort. A cooperative approach, like combining self-regulatory efforts, like the ETA's guideline, are more likely to strike the right balance than the blunt law enforcement action contained in Operation Choke Point.

Another idea is to create a reasonable safe harbor that would allow law-abiding payment companies to report fraudulent merchants to law enforcement without fear of triggering an enforcement action.

ETA stands ready to work with regulators and law enforcement toward our common goal of detecting and eliminating fraud.

Thank you again for the opportunity to testify before the Subcommittee, and I welcome any questions you may have.

[The prepared statement of Mr. Talbott follows:]

Testimony of

The Electronic Transactions Association

Before the

House Committee on the Judiciary

Subcommittee on Regulatory Reform, Commercial and Antitrust Law

Hearing on

"Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point."

July 17, 2014

Testimony Made by

Scott Talbott

Senior Vice President of Government Affairs

The Electronic Transactions Association

Chairman Bachus, Ranking Member Johnson and Members of the Subcommittee, the Electronic Transactions Association (ETA) appreciates the opportunity to submit this statement for the record for the House Judiciary Committee's Subcommittee on Regulatory Reform, Commercial and Antitrust Law's hearing, "Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point."

ETA is an international trade association representing companies that offer electronic transaction processing products and services related to debt, credit, and prepaid cards. The purpose of ETA is to grow the payments industry by providing leadership through education, advocacy, and the exchange of information. ETA's membership spans the breadth of the payments industry, from financial institutions to transaction processors to independent sales organizations to equipment suppliers. More than 500 companies worldwide are members of ETA.

Keeping Fraud Off Payment Systems

ETA strongly supports the vigorous enforcement of existing laws and regulations to prevent fraud. Consumers in the United States choose electronic payments over cash and checks because they have zero liability for fraud, making electronic payments the safest and most reliable way to pay. As a result, payment companies are generally responsible for paying for fraud involving payment systems under Federal law and payment network rules, and thus our members have a strong interest in making sure fraudulent actors do not gain access to payment systems. With the benefit of decades of payment system expertise, ETA members have developed effective due diligence programs to prevent fraudulent actors from accessing payment systems and to terminate access for network participants that engage in fraud. These programs have helped to

keep the rate of fraud on payment systems at remarkably low levels. In 2012, there was more than $4.6 trillion in debit, credit and prepaid card transactions in the United States, but there was only $5.5 billion in credit card fraud. In addition, a recent survey of ETA members indicates that more than 10,000 merchants were discharged last year for fraud. These actions demonstrate the commitment of ETA members to keeping fraudulent actors off payment systems.

Despite this strong record, however, payment processors can never take the place of regulators and law enforcement in protecting consumers. Because regulators and law enforcement can issue subpoenas, conduct investigations, and have far great resources, personnel, and legal authorities, they will always be in a far better position to combat fraud. Yet, payments companies are committed to doing their part.

ETA therefore believes we must be constantly vigilant on continuing to update our processes. The growth of internet commerce has created remarkable new opportunities for business and benefits for consumers, but unfortunately also has created new opportunities for fraud. For example, because websites can change in the blink of an eye, they can be difficult to monitor and easy for fraudsters to exploit. Hence, ETA welcomes further Federal efforts to combat fraudulent activity by unscrupulous merchants that operate on the internet.

In an effort to further strengthen payment systems, ETA has recently published new industry guidelines for merchant due diligence and monitoring that provide more than 100 pages of methods and practices to detect and halt fraudulent actors. The ETA Guidelines were developed by ETA's member companies after months of discussions and sharing of techniques to prevent

fraud. During this process, ETA even shared the preliminary draft guidelines with, and sought comments from, the Federal Trade Commission (FTC), which had strongly encouraged the industry to strengthen its anti-fraud efforts. Now, ETA is actively encouraging its members and companies across the payments ecosystem to make use of the guidelines, especially smaller companies that may not have the resources to develop such advanced practices on their own.

The ETA Guidelines provide a practical and targeted approach to combating fraud on payment systems. ETA members already have a strong commitment to, and financial interest in, keeping fraudulent actors off payment systems, but the targeted nature of the ETA Guidelines gives them enhanced tools to improve their effectiveness and help ensure that law-abiding merchants do not unfairly lose access to payment systems due to overly broad anti-fraud protections.

Another benefit of the ETA Guidelines is that they provide a basis for payments companies to work cooperatively with Federal regulators and law enforcement toward their common goal of stopping fraud. ETA strongly believes that such a collaborative approach is good public policy. It would encourage companies to cooperate with law enforcement by fostering an environment of open communications between government agencies and payments companies. As a result, such a cooperative approach would be more effective at protecting consumers from fraud.

Concerns About Operation Choke Point

Unfortunately, the Department of Justice (DOJ) and other Federal regulators have begun pursuing a more confrontational approach to addressing fraud on payment systems. On March 20, 2013, the Financial Fraud Enforcement Taskforce publicly announced a new initiative by its

Consumer Protection Working Group (which is co-chaired by representatives from the DOJ, the FTC, and the Consumer Financial Protection Bureau) to address mass consumer frauds by holding banks and payment processors liable for the acts of certain merchants.[1] This initiative, named "Operation Choke Point" by the DOJ, aims to "close the access to the banking system that mass marketing fraudsters enjoy – effectively putting a chokehold on it."[2]

Although ETA strongly supports increased law enforcement aimed at preventing mass frauds, it has serious concerns about the Operation Choke Point approach. In ETA's view, Operation Choke Point employs the wrong legal tools, is unnecessarily confrontational, and creates serious risks to law abiding processors and merchants without producing any benefits to consumers beyond those which could be obtained with a more focused and collaborative approach.

The DOJ has sought to implement Operation Choke Point by initiating investigations and civil suits under the Financial Institutions Reform, Recovery, and Enforcement Act, 12 U.S.C. § 1833a (FIRREA). Under FIRREA, the DOJ can initiative investigations and bring civil suits for alleged violations of 14 predicate criminal offenses, including wire fraud "affecting a federally-insured financial institution."[3] Several courts have recently held that FIRREA suits can be brought against not only third parties whose violations "[affect] a federally-insured financial institution," but also against the banks whose violations affect themselves.[4] This broad reading of FIRREA has given DOJ a very powerful tool because under FIRREA the statute of limitations

---

[1] http://www.justice.gov/iso/opa/doj/speeches/2013/opa-speech-130320.html.
[2] *Id.*
[3] 12 U.S.C. § 1833a(c)(2).
[4] United States v. Bank of New York Mellon, 941 F. Supp. 2d 438 (S.D.N.Y. 2013); United States v. Countrywide Fin. Corp., 961 F. Supp. 2d 598 (S.D.N.Y. 2013); United States v. Wells Fargo Bank, N.A., 972 F. Supp. 2d 593 (S.D.N.Y. 2013).

is 10 years and cases only need to be proven by "preponderance of the evidence," rather than the "beyond a reasonable doubt" standard required in criminal prosecution.[5] In addition, FIRREA provides for penalties of up to $5 million for each violation or, if greater, the amount of any pecuniary gain derived by the violation or of any losses inflicted on another person.[6] These provisions significantly tilt the litigation playing field in favor of the DOJ and make FIRREA cases very costly for companies to defend against and risky to litigate.

It is important to note that FIRREA was not designed to address mass frauds. It was passed to reform the regulatory regime for thrifts in the wake of the S&L Crisis of the 1980s. The purpose of Section 1833a was to protect the government from financial frauds. Hence, Section 1833a provides the Federal government with enhanced authority to pursue claims against individuals for fraudulent actions that directly harm the Federal government or harm financial institutions insured by the Federal government. It is not a consumer protection statute, which is demonstrated by the fact that FIRREA penalties do not redress consumer injury, but instead get paid to the U.S. Treasury. Therefore, the use of FIRREA for consumer protection purposes is a case of the wrong tool being used for the right goal.

Although no court has yet issued a final decision in a FIRREA case involving payment processing, DOJ has recently settled two FIRREA cases involving payment processing and issued scores of subpoenas to financial institutions as part of Operation Choke Point. These settlements, combined with recently released DOJ memoranda detailing the agency's plans for Operation Choke Point, have raised concerns among ETA's members that Operation Choke Point

[5] 12 U.S.C. § 1833a(f), (h).
[6] 12 U.S.C. § 1833a(b).

will result in the government seeking to broaden the scope of processor liability for the acts of merchants.[7] There is also concern that Operation Choke Point will be used to impose penalties on financial institutions for processing transactions of certain categories of legal but disfavored businesses.

The problems with Operation Choke Point are not limited to the DOJ. ETA is also concerned that other Federal regulators are considering following the DOJ's lead and adopting additional initiatives modeled on Operation Choke Point. ETA's members have reported a sharp increase in information requests and civil investigative demands from the FTC. In light of the DOJ's implementation of Operation Choke Point and recently released DOJ memorandum indicating FTC involvement with the development of Operation Choke Point, the FTC's increased interest in payment processing has sparked concerns that the FTC has begun its own Operation Choke Point. [8]

Currently, the FTC can assert jurisdiction over payment processors that engage in unfair or deceptive acts or practices in violation of Section 5 of the Federal Trade Commission Act, and violations of the Telemarketing Sales Rule.[9] The FTC also can bring cases against payment processors for "assisting and facilitating" a merchant's violations of the Telemarketing Sales

---

[7] The Department of Justice's "Operation Choke Point": Illegally Choking Off Legitimate Businesses?, U.S. House of Representatives, Committee on Oversight and Government Reform, Staff Report (May 29, 2014), Appendix 1.
[8] *Id.* (The DOJ has indicated that it is making "significant efforts to engage other agencies," including the FTC. The DOJ also has noted that "[t]he FTC's efforts in this area predate our own, and not surprisingly our agencies work closely together." (Memorandum dated November 21, 2013 to Staff of the Office of the Attorney General et. al. from Maame Ewusi-Mensah Frimpong, Deputy Assistant Attorney General, Civil Division. Subject: Operation Choke Point, p. 12)).
[9] 15 U.S.C. § 45; 16 C.F.R. § 310.

Rule, but such liability only applies if a payment processor "knows or consciously avoids knowing" that the merchant violated the rule. [10]

ETA fully supports the proper enforcement of these statutes by the FTC, but is concerned that the FTC is looking to change its long-standing policy of pursuing only processors that were actively engaged in assisting a merchant in committing fraud or avoiding detection. To the extent the FTC begins premising liability on nothing more than providing a merchant an account, or deems high return rates to be constructive knowledge of fraud, it will be dramatically altering the liability scheme for payment processing in a manner that could have significant, adverse consequences.

Impact of Operation Choke Point on Processors, Entrepreneurs, and Consumers

From a public policy perspective, Operation Choke Point and any similar efforts by the FTC or other regulators to impose enhanced liability on payment processing will likely have adverse consequences for not only merchants and entrepreneurs, but also the very consumers Operation Choke Point purports to protect. In addition, Operation Choke Point sets a troubling precedent of government agencies using the payment systems to achieve objectives unrelated to preventing financial fraud.

First, if payment companies' liability for the actions for merchants increases, processors may very well have little choice but to increase the prices of payment services for merchants and/or restrict access to their payment systems to manage their new liability exposure. Invariably, the

[10] 16 C.F.R. § 310.3

brunt of these burdens will fall on small, new and innovative businesses because they pose the highest potential risks. For example, start-up internet businesses with liberal return policies present high risks to financial institutions because they have no transaction history, rely on card-not-present transactions and have (by design) high return rates. Federal regulators view high return rates as strong evidence of fraud. Due to the risks these new businesses present, banks and payment processors may very well decide that the increased liability risks outweigh the benefits of having them as customers. Because in today's marketplace consumers expect merchants to accept debit, credit, and prepaid cards, the inability of a merchant to access the payment systems could effectively be the death knell for its business. New restrictions on access to payment systems, or even higher costs to access payment systems, could therefore become an impediment to job creation and innovation, especially in the critical high-tech start-ups and internet commerce segments of the economy.

Second, increasing liability on payment processing, especially processing of debit, credit, and prepaid cards, does not necessarily benefit consumers. It is consumers who will ultimately pay for the higher costs arising from increased liability. They also will be harmed by the inconvenience of not being able to use their preferred methods of payment (credit, debit, and prepaid cards) with some merchants due to more restrictive access to payment systems. Similarly, they would be harmed if new liability on processors impedes continued innovations in electronic payments. Over the last twenty years, electronic transactions have grown rapidly to become the dominant method of payment for consumer transactions due to their convenience, security (especially when compared to cash), and customer service. Therefore, to the extent that

new liability risks impede the evolution of electronic transactions, consumers will have less access to the payment methods they prefer and beneficial developments in electronic payments.

Third, there is a real risk that a confrontational approach, like Operation Choke Point, will alter payments companies' natural incentive to cooperative with law enforcement and regulatory authorities if they believe that such cooperation will only result in enforcement actions against them. Thus, a far better approach would be to establish a reasonable safe harbor that would allow payments companies, which were not directly involved in the fraudulent activities of a merchant, to work with regulators without any risk of triggering an enforcement action. ETA believes that such cooperation between payments companies and regulators is likely to be more effective because it recognizes and further strengthens the strong incentives such companies already have to prevent fraudulent actors from accessing payment systems. This conclusion (as well as further analysis of the adverse consequences arising from imposing additional liability on payment processors) was also the result of a recent study by NERA Economic Consulting commissioned by ETA, which is attached as Exhibit A.

Finally, enforcement actions against payment systems are an inappropriate tool for regulators to use to limit the ability of consumers to access legal but currently disfavored industries. There has been much debate about the attempts by Operation Choke Point and similar regulatory efforts to compel payments companies to sever relationships with a variety of legal but disfavored industries, ranging from coin dealers and short-term lenders, to home-based charities and pharmaceutical sales.[11] ETA believes that such efforts unfairly expose institutions to

[11] *See* The Department of Justice's "Operation Choke Point": Illegally Choking Off Legitimate Businesses?, U.S. House of Representatives, Committee on Oversight and Government Reform, Staff Report (May 29, 2014), p. 8.

regulatory actions merely for engaging in lawful commerce. Moreover, if the precedent is set that regulators can unilaterally intervene to keep certain lawful industries off payment systems, payments companies will be subject to shifting regulatory exposure as the disfavored industries of regulators shifts with changes in administrations and agency personnel. If regulators have concerns about a particular industry, the appropriate forums for addressing those concerns are formal rulemakings, Congress, or state legislatures. To be clear, ETA takes no position on which types of industries should be legal and its members are fully committed to preventing any businesses engaged in activities prohibited by statute or regulation from accessing payment systems. ETA merely seeks to ensure that payments companies can freely process transactions for any law-abiding merchant.

Conclusion

Operation Choke Point is premised on the flawed assumption that increasing liability on lawful payments companies for the actions of fraudulent merchants will yield only benefits to consumers. In practice, however, imposing new liability standards on such institutions is likely to have serious adverse consequences for not only law-abiding merchants, but also consumers generally. There needs to be a careful balancing of the need to limit access to payment systems to prevent fraud and the need to ensure that all law-abiding businesses can access the payment systems consumers want to use. A cooperative approach to combating fraud by financial institutions and Federal regulators is far more likely to strike the right balance than blunt enforcement actions. Accordingly, ETA stands ready to work with federal regulators to work cooperatively toward our common goal of preventing fraud.

Mr. BACHUS. Mr. Thompson.

TESTIMONY OF DAVID H. THOMPSON, MANAGING PARTNER, COOPER & KIRK, PLLC

Mr. THOMPSON. Mr. Chairman, Ranking Member Johnson, and Members of the Subcommittee, thank you very much for including me on this panel today.

The Department of Justice, working with the FDIC, the OCC, and the Fed have conspired to choke off and strangle legitimate businesses by depriving them of access to the financial system. Many of the victims of Operation Choke Point are legitimate businesses.

These agencies have undertaken this operation without any Congressional authorization and, although they may disapprove of these industries, neither the FDIC nor the OCC nor the Fed have any power to shut down lawful businesses. They can ensure the safety and soundness of banks, but they have no authority to condemn wholesale lawful industries.

To make matters worse, the Department of Justice and the banking agencies have failed to provide these law-abiding companies with any opportunity to be heard and to defend themselves. Instead, they have acted through back-room—a back-room campaign of veiled threats and regulatory intimidation.

I come to you today on behalf of the Community Financial Services Association of America, the leading trade association for short-term credit providers, and its members have been targets of Operation Choke Point.

It is important to understand the mechanism by which these agencies have brought about their desired result. The banking agencies have targeted disfavored industries by expanding the definition of reputational risk. This is the club that they yield and wield.

The agencies had previously and consistently defined the concept of reputational risk to refer specifically to the risk of a bank's reputation that arose from its own services and its own products. A bank's reputation could suffer, in other words, if it provided substandard products or services.

But the agencies had never before held—said that a bank needed to assess the reputation of its customers as part of its management. Banks ensured their good reputation by meeting the needs of their customers, not by judging the popularity of their customers.

This is, of course, not to say that a bank had no need to evaluate its customers. A bank is required to have procedures in place that ensure that it does not engage in illegal activity or facilitate the commission of crimes by its customers. This risk is encompassed under the rubric of compliance risk, however, not that of reputation risk.

A bank was never required before to have procedures in place to ensure that it did not have customers who, though lawfully engaged in demonstrably lawful businesses, might simply be unpopular with the public or with the current Administration.

In imposing this new interpretation of reputation risk upon the banking industry, the agencies have consistently chosen to proceed

without providing the public with notice and an opportunity to comment, and this is a fatal flaw in this regulatory regime.

It violates the Administrative Procedures Act. It violates the due process clause. And these violations have real-world consequences. Members of the association I represent have had scores of banking relationships severed in the aftermath of Operation Choke Point.

And the key point to understand is that these relationships have been long-standing. They have harmoniously coexisted with safety and soundness requirements and anti-money laundering regimes. And now over 80 banks have severed these relationships. Lightening might strike in the same place twice on occasion, but it doesn't strike 80 times over and over and over again by coincidence.

And something has changed. It is not the return rates of the short-term lending industry. It is not their return—their risk profile. There is nothing in the free market that has changed. It is Operation Choke Point that has changed. That is the driving force behind these decisions.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Thompson follows:]

STATEMENT OF DAVID H. THOMPSON

Managing Partner, Cooper & Kirk, PLLC

Before the U.S. House Committee on the Judiciary,

Subcommittee on Regulatory Reform, Commercial and Antitrust Law

Concerning

"Guilty until Proven Innocent?

A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point"

July 17, 2014

Chairman Bachus, Ranking Member Johnson, and Members of the Subcommittee. Good morning, and thank you for inviting me to participate in today's hearing on "Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point." I am honored to be included among the distinguished members of this panel, and I am pleased to be able to share with you today my thoughts on the deeply-troubling legal issues that are raised by the Department of Justice's ("DOJ") Operation Choke Point.

DOJ is now using against legitimate American businesses tactics that are strikingly similar to those that have been used against corrupt foreign institutions serving terrorists. Working with DOJ, the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of the Currency ("OCC"), and the Board of Governors of the Federal Reserve System ("the Board") have conspired to choke off and strangle legitimate businesses by depriving them of their access to the financial system. Many of the victims of Operation Choke Point are law-abiding companies, ranging from coin dealers to dating services. With their ability to open a bank account or even to deposit a check now taken from them, these law-abiding companies are being deprived of their right to pursue their chosen trade and of their very right to exist.

DOJ has undertaken this operation without any Congressional authorization. Although they may disapprove of these businesses, neither FDIC, nor OCC, nor the Board has the power to shut the industry down, or even significantly restrict it, through ordinary, legal means. The statutes under which these three agencies perform their regulatory duties authorize them to ensure the safety and soundness of the banks. While these agencies have the authority to police the banking system, they have no authority to judge and condemn whole industries as unworthy

of access to that banking system. It is neither surprising nor unreasonable that Congress has not delegated such sweeping power.

To make matters worse, DOJ and the banking agencies have failed to provide these law-abiding companies, including short-term credit providers, with any opportunity to be heard and to defend themselves against these scurrilous accusations and slanders. The agencies have chosen to proceed not through notice and comment rulemaking nor through any procedure that would expose their operation to the oversight of the Congress; they have acted instead through a back room campaign of veiled threats and regulatory intimidation. They have made no effort to distinguish those who are breaking the law from those who are making every effort to comply with not only the letter but also the spirit of our consumer protection laws. In sum, Operation Choke Point is unconstitutional, unlawful, and simply un-American.

I. The Short-Term Credit Industry Meets the Needs of America's Underserved Communities.

I come before you today to speak on behalf of the Community Financial Services Association of America (CFSA), the leading trade association representing short-term credit providers. The Association and its members provide short term loans that help consumers, many of whom are underserved, make ends meet in today's difficult economic conditions. These loans are typically the equivalent of an advance on the borrower's paycheck or other source of regular income. They provide a type of short-term credit to over nineteen million American households, helping to bridge the unexpected financial needs that often arise between income installments.

A short-term, small dollar loan is a convenient and reasonably-priced vehicle for short-term financial needs, often cheaper than overdraft fees and late fees on credit cards or utility bills. Many short-term credit providers offer other financial services to their customers, including bill payment, check cashing, installment loans, and prepaid debit cards. Like short-

term small dollar loans, these lines of business serve critical needs in underserved communities. Members of these communities often cannot obtain any service from a bank or can obtain those services only at costs far higher than would be charged by a short-term credit provider. Furthermore, customers want these products, as they believe they are cost competitive and effective and are satisfied with their experiences with short term credit providers. According to a Harris poll of CFSA members' customers conducted in 2013, well over 90 percent expressed satisfaction with the terms (96%) and cost (92%) of their short-term small-dollar loans, had found that those loans provided a valuable safety net during times of unexpected financial difficulty (95%), and believed that they should be free to take out such a loan without government interference (95%).

Both the Congress and the State legislatures have recognized the importance of short-term small-dollar loans and the potential consequences of their misuse. As a result, most States—oftentimes acting in consultation with and with the cooperation of the trade associations that represent the short-term credit industry—have passed robust consumer protection laws to ensure that loans are offered and consumed responsibly. These laws require licensing to specifically authorize these lenders to operate in their state, may cap the amount of the loan or its fees, limit the number of times a consumer may renew a loan, and/or require certain disclosures. Every member of the CFSA must hold a license and comply with the laws in every state in which they maintain a storefront location and in every state in which their online customers reside. The federal consumer financial protection laws also apply to these lenders, including TILA, ECOA, EFTA, FCRA, and UDAAP. Notably, the Truth in Lending Act, 15 U.S.C. § 1601 et seq., requires full disclosure of the costs and terms of the loans in order to ensure that consumers have

the information they need to make responsible borrowing decisions. Short-term credit providers are frequently examined by state regulators and by the CFPB.

Short-term credit providers of necessity rely on banking services to operate. When a prospective borrower applies for the loan—at a storefront location, or online—he or she typically provides a post-dated check or an electronic debit authorization for the value of the loan, plus a fee. The lender immediately advances the customer funds, then after a specified period of time, usually determined by the customer's next payday, the borrower returns to repay the loan and fee. But if the customer does not return, the terms of the transaction permit the lender to deposit the post-dated check or to execute the debit authorization. In order to have that security, the lender must have a deposit account with a bank and/or access to the Automated Clearing House (ACH) network.

It is their reliance on the banks for conducting their businesses that made short-term credit providers an easy first target for DOJ's campaign against lawful businesses who are disfavored by the current administration. Lacking the legal authority to regulate short-term credit providers, FDIC, OCC, and the Board have, in coordination with DOJ, conducted a campaign of extra-legal regulation, first imposing an expanded standard of reputation risk on the industry and then using that standard to threaten banks who do business with short-term credit providers. It is about the legal and, specifically constitutional, concerns that are raised by this campaign of de facto regulation and administrative intimidation that I would like to speak with you today.

II. The Ever-Expanding Regulatory Definition of "Reputation Risk."

The agencies have the authority under the Federal Deposit Insurance Act to ensure the safety and soundness of the banking industry. See 12 U.S.C. § 1831p-1. In performing their statutory duty, the agencies have required that the banks have adequate procedures in place to assess and manage risk.[1] Among the specific risks that a bank must manage is the risk that its reputation may become tarnished in the eyes of the public.

The agencies had previously and consistently defined the concept of "reputation risk" to refer specifically to those risks to a bank's reputation that arose from the products and services provided by the bank itself and by third parties with whom a bank contracted for the provision of those products and services. A bank's reputation could suffer, in other words, if it provided or seemed to provide poor products and poor service to its customers.

The agencies had never before held that a bank needed to assess the reputation of its customers as part of its management of reputation risk. Banks insured their good reputation by meeting the needs of their customers, not by judging the popularity of their customers.

This is, of course, not to say that a bank had no need to evaluate its customers. A bank is required to have procedures in place that ensure that it does not engage in illegal activity or facilitate the commission of crimes by its customers; this risk is encompassed under the rubric of compliance risk, however, not that of reputation risk. A bank was never before required to have procedures in place to ensure that it did not have customers who, though lawfully engaged in

[1] The agencies have identified several such risks that a depository institution must manage. These include credit risk, market risk, liquidity risk, operational risk, and compliance risk. See, e.g., FRB, Supervisory Letter: Risk-focused Safety and Soundness Examinations and Inspections. SR 96-14 (May 24, 1996).

demonstrably lawful business pursuits, might simply be unpopular with the public or with the current administration.

Although DOJ is now using FDIC, OCC, and the Board to wage its covert campaign against disfavored industries and businesses, these three agencies had already for some time been expanding their regulatory power through a gradual process of interpretive redefinition of the concept of reputation risk. They carried out this process of incremental self-aggrandizement by progressively unmooring the concept of reputation risk from its traditional definition within the banking industry.

For example, in the summer of 2011, FDIC published a Supervisory Insight article entitled "Managing Risks in Third-Party Payment Processor Relationships." The article warns banks of heightened risks, including reputation risks, associated with doing business with certain types of merchants, including online payday lenders. FDIC, Managing Risks in Third-Party Payment Processor Relationships, SUPERVSIORY INSIGHTS, Summer 2011, at 3. For the first time, the article offers a list of 30 merchant categories, including online payday lending and numerous other lawful businesses that the agency has deemed to involve "high-risk" activity. The Department of Justice has acknowledged, in response to legislative investigations of Operation Choke Point, that FDIC developed this list of "high-risk merchants" for purposes related to regulating the banking industry. Letter from Peter J. Kadzik, Assistant Attorney General, U.S. Department of Justice, Office of Legislative Affairs, to the Honorable Tim Johnson, Chairman, Committee on Banking, Housing, and Urban Affairs, U.S. Senate, 4 (June 24, 2014). The article further urges banks to be wary of customers with high aggregate return rates and those that bank with more than one financial institution. *Id.*

In imposing this new interpretation of reputation risk upon the banking industry, the agencies have consistently chosen to proceed without providing the public with notice and an opportunity to comment. Furthermore, these agencies provide no objective criteria for measuring reputation risk or for distinguishing between law-abiding, responsible bank customers and bank customers that engage in fraudulent or otherwise unlawful financial practices. Far from tailored guidance that would aid banks in targeting those customers who are engaged in fraudulent or otherwise unlawful practices, the agencies have created a vague and subjective standard that can be used to pressure banks to cut off relations with law-abiding customers engaged in any line of business that is disfavored by DOJ.

The opportunity for abuse that is inherent in such a subjective and pliant standard is patent. Under the guise of protecting the safety and soundness of banks, FDIC, OCC, and the Board are now using this newly defined concept of reputation risk to wage a covert war against certain legitimate businesses that rely on banking services to function and that are disfavored by this administration, including short-term credit providers.

III. The Agencies Are Imposing Regulations on the Banking Industry Without Statutory Authority and Without Observing the Procedural Requirements of the Administrative Procedure Act.

In order to play their part in Operation Choke Point, the agencies are relying extensively on their redefinition of reputation risk, a concept now transformed into one that requires a bank to assess the reputations of each and every one of its customers and to refuse to do business with those customers whom, in the judgment of the regulators, the public might disfavor. The implementation of this new standard has been carried out without statutory authorization and without observing the procedures required by the Administrative Procedure Act.

The Administrative Procedure Act requires that agency actions be set aside when they are conducted "without observance of procedure required by law." 5 U.S.C. § 706(2)(D). Before it may promulgate a binding rule or substantially revise a previously announced interpretation, an agency must provide public notice in accordance with law and "give interested persons an opportunity to participate in the rule making through submission of written data, views, or arguments with or without opportunity for oral presentation." 5 U.S.C. § 553(b), (c).

The agencies failed to provide any sort of notice and opportunity to comment in advance of promulgating the rules relating to their new definition of reputational risk. These documents do more than merely announce "interpretative rules and statements of policy"; they have been and are being enforced by the banking agencies to create new legal obligations for banks wishing to do business with the entities described in guidance documents, including short-term credit providers.

Reputation risk—the fulcrum for Operation Choke Point—is no longer limited to the risk that negative publicity regarding a financial institution itself or third parties who provide services in its name will cause a decline in customer base, costly litigation, or loss of revenue. Reputation risk has now been redefined and remade into a concept that is vague, manipulable, and wholly foreign to customary bank examination practices.

As redefined, reputation risk could "ostensibly be invoked to compel a depository institution to sever a customer relationship with a small business operating in accordance with all applicable laws and regulations but whose industry is deemed 'reputationally risky' for no other reason than that it has been the subject of unflattering press coverage, or that certain Executive Branch agencies disapprove of its business model." Letter from Rep. Jeb Hensarling, Chairman, H. Comm. on Fin. Servs., to Janet Yellen, Chair, The Fed. Reserve Sys. (May 22, 2014). "The

introduction of subjective criteria like 'reputation risk' into prudential bank supervision can all too easily become a pretext for the advancement of political objectives, which can potentially subvert both safety and soundness and the rule of law." *Id.*

The requirements of the Administrative Procedure Act are not mere technicalities. Notice and comment rulemaking ensures that an agency will consider the ramifications of what it is doing, address the concerns of the regulated industry and of other interested parties impacted by the regulation, and adequately explain its statutory authority and its expert rationale.

Notice and comment rulemaking was devised by Congress in order to make sure that an agency does not adopt irrational, arbitrary, and capricious rules. The failure to make use of this statutorily-required procedure has here resulted in a rule that is vague, malleable, standardless, and open to misunderstanding, misapplication, and simple abuse. In promulgating their new definition of reputation risk, the Agencies' have created precisely the sort of defective rule that notice and comment rulemaking was designed to prevent.

Of perhaps even greater concern, this novel definition of reputation risk has untethered the agencies from their statutory source of authority, making them no longer prudential regulators of American financial institutions, but the legal and reputational police of American society. As documents uncovered in recent investigations of Operation Choke Point confirm, short-term credit providers are only the first in a long series of businesses which the government now intends to target for extermination on the ground that they are "reputationally risky" in the eyes of the FDIC, OCC, the Board, and DOJ.

IV. The Agencies Have Deprived Americans of Their Liberty Without the Due Process of Law Required by the Fifth Amendment to the Constitution.

The Fifth Amendment to the Constitution guarantees that no person will be deprived of life, liberty, or property without due process of law. In their effort to advance their agenda, FDIC, OCC, and the Board have each violated this basic tenet of constitutional jurisprudence. Short-term credit providers have been the first industry to be stigmatized, branded, barred from pursuing their chosen line of business, and deprived of their banking relationships without any notice or opportunity to be heard and to defend their right to exist.

As an initial matter, the agencies have inflicted grave reputational harm upon CFSA's members and other law-abiding responsible short-term credit providers by stigmatizing them as "illegitimate," "fraudulent," and "high risk." They gave no notice to the industry of their judgment. They gave the industry no opportunity to be heard. They simply announced to the banks which they regulate that they had decided that short-term credit providers are "fraudulent." Under Operation Choke Point, sentence is now being passed and carried not only without due process of law but without regard for the guilt or innocence of the accused.

This stigma that the banking agencies have branded upon the law-abiding and responsible short-term credit providers now threatens to preclude them from pursuing their chosen line of business. Indeed, to choke off these businesses from the financial services that they must have in order to pursue their chosen line of business is the precise purpose of the agencies' actions, a purpose openly declared in the very name that the government has chosen for its unlawful enterprise: Operation Choke Point. America's short-term credit providers have been deprived of their right to continue to exist without having been provided any notice or having been afforded any opportunity to be heard.

Further, by attacking the reputations of short-term credit providers, the agencies have effectively coerced financial institutions to cease providing them with bank accounts and other essential financial services. The agencies have thus deprived these lenders of tangible benefits and interests that they had previously possessed. Again, they have done so without providing the process due under the law.

The behavior of these agencies and of DOJ in their conducting of Operation Choke Point has fallen well short of the requirements of the law of our land. Put simply, Operation Choke Point is patently, flagrantly, and intolerably un-American. This is not how law is made and enforced in America. This is not how justice is served in our society.

V. The Casualties of Operation Choke Point.

DOJ and the three banking agencies may claim that the aim of Operation Choke Point is to choke off only "fraudsters" and unlawful businesses, but the actual results of Operation Choke Point prove otherwise. The vague and malleable standard of reputation risk has provided banks with no guidance on how to discriminate between lawful and unlawful enterprises. Faced with the thinly-veiled threats of the banking regulators and the tactics of intimidation and prosecutorial bullying, the banks have had no choice but to yield to the coercion of their regulators and terminate those customers who failed to curry the favor of the administration. This concerted campaign has had the result, therefore, of sweeping away the members of the short-term credit industry without regard for guilt or innocence.

As a growing number of banks have terminated their relationships with law-abiding, licensed, and responsible short-term credit providers, these businesses must each day wonder when the government will terminate their remaining banking relationships and must compete for

service within the ever shrinking pool of banks who remain committed to their mission of providing customer service and are willing to stand up to regulatory bullying.

I will offer a few examples of the damage that Operation Choke Point has already done to the short-term credit industry. One lender, Advance America, has lost longstanding and positive business relationships with at least nine banks as a result of Operation Choke Point. Hancock Bank and Whitney Bank informed Advance America of their intention to close its accounts on the ground that they were "unable to effectively manage [the lenders'] Account(s) on a level consistent with the heightened scrutiny required by [their] regulators . . . ." Fifth Third Bank wrote that it would stop doing business with short-term credit providers altogether on the ground that the entire industry is "outside of [its] risk tolerance." Synovus Bank and Umpqua Bank likewise terminated Advance America's accounts. At least two of Advance America's banks expressed regret and explained that the service terminations were the result of pressure from their prudential regulator. Cadence Bank also terminated Advance America's accounts without explanation. Advance America has not been able to find local banks to service certain stores that were affected by the terminations; many of the banks it contacted for that purpose had decided to exit the short-term small-dollar industry entirely due to regulatory pressure. No bank expressed a concern about Advance America; every bank based its determination on a sweeping judgment of the industry as a whole, an irrational judgment they were compelled to make by their regulator.

Another CFSA member, Cash Tyme, has received termination notices for its accounts at three financial institutions. Two alluded to the regulatory environment. Fifth Third Bank informed Cash Tyme, as it had informed Advance America that the entire industry was "outside [its] risk tolerance." Regions Bank informed Cash Tyme that it "ha[d] chosen to end relationships with certain types of customers deemed to be high risk." Cash Tyme has been

unable to find substitute banks to service certain stores affected by the terminations, nor has it been able to find a bank that will provide ACH services.

CFSA Member Speedy Cash, Inc. (Lending Bear), after a seventeen year banking relationship, also received a termination notice from Bank of America. A bank officer told Speedy Cash, Inc. that Bank of America was "exiting the payday advance space," expressed regret at the decision, and led it to believe that the termination decision depended only on Speedy Cash Inc.'s classification as a short-term credit provider. Indeed, Speed Cash recently received a formal notice from Bank of America that its small business accounts would soon be closed "based on the nature of your business and associated risks." Furthermore, two of its current banking partners now refuse to open new accounts for Speedy Cash, Inc.

CFSA member Xpress Cash Management likewise received a termination notice from Fifth Third Bank that explained that the short-term small-dollar loan industry is "outside [its] risk tolerance."

The foregoing specific examples of banks that have terminated their relationships with CFSA members as a result of regulatory pressure are merely illustrative of the severely harmful effects of Operation Choke Point on the short-term credit industry. Numerous other CFSA members have lost longstanding, positive banking relationships, despite their law-abiding and responsible business practices.

The agencies and DOJ knew early on that their coordinated, coercive campaign of backroom pressure tactics was succeeding in prompting banks "to exit or severely curtail" business with all short-term credit providers, and that "banks may have therefore decided to stop doing business with legitimate lenders." Six-Month Status Report Mem. at 10.

Because short-term credit providers cannot survive without access to banking services, Operation Choke Point has begun to have its intended and necessary effect. As one internal DOJ memorandum noted, "a large Internet payday lender decided recently to exit the business due to difficulties securing a bank or payment processor relationship." Memorandum from Michael S. Blume, Dir., Consumer Prot. Branch of U.S. Dep't of Justice, to Stuart F. Delery, Principal Deputy Ass't Att'y Gen., Civil Div. of U.S. Dep't of Justice 2 (July 8, 2013), in COMM. REP. ON OPERATION CHOKE POINT app. at HOGR-3PPP000166. The regulators celebrated "this type of positive conduct." Six-Month Status Report Mem. at 6, 10.

Violating basic principles of due process should not be a cause for celebration. These agencies should put an end to the lawlessness engendered by Operation Choke Point and end the unfair targeting of lawful businesses and entire industries.

Mr. BACHUS. Thank you, Mr. Thompson.
Mr. Weinstock.

TESTIMONY OF PETER WEINSTOCK, PARTNER, HUNTON & WILLIAMS LLP

Mr. WEINSTOCK. Chairman Bachus, Ranking Member Johnson, and Members of the Subcommittee, the U.S. Department of Justice created Operation Choke Point ostensibly to combat consumer fraud. However, it has become apparent that the program instead seeks to irradiate disfavored business.

To do so, the program uses aspects of FIRREA to threaten injunctions and civil penalties against banks that provide access to the payment system for certain merchants and payment processors to whom they provide services.

Without access to the banking and payment systems, these entities are unlikely to continue operating. This was precisely the DOJ's goal from the outset.

Banks are disassociating with customers engaged in lawful behavior, not simply customers whose activities may be fraudulent, as bankers try to define the next targets of the DOJ's efforts.

The DOJ even acknowledged the prospects for such parties' banking relationships to be collateral damage to its initiative.

With Operation Choke Point, the DOJ is starting from the premise that certain lines of business or industries are anathema and then working backward to find legal violations.

Using FIRREA to implement Operation Choke Point, the government can issue subpoenas, take depositions, and seek civil damages against entities committing wire fraud or mail fraud, affecting Federally insured depository institutions. In doing so, the DOJ need only meet the lower evidentiary burden of proof by a preponderance of the evidence to demonstrate fraud.

The DOJ's objective, however, is not to bring any action against those suspected of committing fraud, but to cause banks to "scrutinize their account relationships and, if warranted, to terminate fraud-tainted processors and merchants."

As a result of the DOJ's use of FIRREA, banks have been forced to choose between, at a minimum, incurring significant discovery and compliance costs and potentially accepting costly penalties, on one hand, or terminating existing relationships with processors and merchants, on the other hand, even if they are operating lawfully.

The DOJ has calculated the bank's sensitivity to the costs of responding to the DOJ's inquiries, let alone to civil and criminal liability and regulatory action. Their goal is to cause a bank to "scrutinize immediately its relationships with processors and fraudulent merchants and to take necessary action," i.e., to cut them off.

In Operation Choke Point, the determination of whether a merchant is fraudulent is determined by the DOJ based on a line of business rather than by any adjudication where those who are accused are afforded due process.

DOJ believes that legitimate banks will become aware of perhaps unrecognized risks and corrupt banks will be exposed. In other words, a bank that does not agree with the DOJ's assessment, perhaps based only on return rates and violations of State laws which

the DOJ concedes is only a red flag of potential fraud, will deem to be corrupt and subject to legal action.

Operation Choke Point has had a chilling effect on banks' willingness to transact business with processors and merchants where the reward cannot compensate enormous costs and potential exposure.

FIRREA was passed in response to the savings and loan crisis. The goal of FIRREA was to make those who committed outright fraud and insider abuse against depository institutions pay the price for those actions. The DOJ is clearly stretching the limits of FIRREA in the context of Operation Choke Point.

With the current analysis by the DOJ, intent is turned on its head. Instead of using FIRREA to protect banks from fraud, the DOJ is prosecuting banks for conduct disfavored in businesses that are disfavored using discovery and draconian subpoena power. Entities shut out of one bank have little hope of establishing a subsequent banking relationship and will become defunct without an opportunity to defend themselves.

While I am not championing the efficacy of payday lending, there are undoubtedly some organizations that operate lawfully and provide un-bank customers with a service that such customers believe is valuable, certainly one less dangerous than engaging a loan shark.

Indeed, a review of the development of Operation Choke Point reveals the DOJ's new technique. As noted by internal memoranda on Operation Choke Point, the DOJ's primary target is the short-term lending industry.

Brandishing FIRREA as a sword, DOJ chose to go after a number of banks that were doing business with third-party payment processors to get them to cease providing services to those entities.

DOJ stunningly proposed identifying ten suspect banks for analyzing return rate data, among other criteria. However, the DOJ's standard for identifying fraud was arbitrary and relied almost exclusively on NACHA average return rates and potential violations of State law.

NACHA does not define a 3 percent level. NACHA does have a 1 percent level for unauthorized transactions as an indicator of fraud. NACHA doesn't have a level for not sufficient funds.

The chilling effect of Operation Choke Point is not limited to DOJ actions. Instead, it is partially predicated on the notion that reputation risk arises when banks transact business with processors and high-risk merchants. What constitutes reputational risk, however, is not clearly defined.

The FDIC issued a financial institution letter that explains reputation risk as a risk arising from negative public comment and adds any negative publicity involving the third party, whether or not the publicity is related to the institution's use of the third party, could result in reputation risk.

Sarah Raskin, Federal Reserve Board Governor, explained reputation risk in a speech as the risk to enterprise value from—to brand recognition and customer loyalty. Raskin further added that supervision of banks is necessary in order to prevent the accumulation of reputation risk to the extent it constitutes a hidden exposure.

These comments illustrate the vague and subjective standard now being wielded by the Federal Government against banks who are doing business with disfavored industry. The guidance plainly does not distinguish between lawful and fraudulent activity.

Reputational risk is not legal risk. Regulatory authorities proffer no standard of how to evaluate whether, as Raskin states it, that reputation risk is accumulating and that any exposure is material to safety and soundness.

The OCC and the Fed in the fourth quarter of last year issued guidance on third-party risk that requires financial institutions to risk-assess their customer base and to engage in extensive review of the compliance management systems of their customers. In effect, bankers now have to police their customers' compliance management systems.

This goes well beyond the BSA's know-your-customer requirements. This gets into the burden on banks to police whether customer—disclosures to their customers are deceptive, whether customers are engaging in improper activity.

Basically, they have to police all of their customers' activities. What cost is that imposing on third parties? What cost when the third parties have to have bank-like compliance management systems? And what is that going to do to our economy?

So, undoubtedly, there is a chilling effect going on. Bankers are trying to evaluate high-risk customers and then determine which of those will be next on the regulatory or government list and then terminate them. Bankers are making the business decision to de-risk their customer base accordingly.

Thank you.

[The prepared statement of Mr. Weinstock follows:]

Legal Ramifications of Operation Choke Point

By Peter Weinstock, Hunton & Williams LLP[1]

I. Background

The U.S. Department of Justice ("DOJ") created Operation Choke Point ostensibly to combat consumer fraud.[2] However, it has become apparent that the program instead seeks to eradicate disfavored businesses. To do so, the program uses aspects of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 ("FIRREA")[3] to threaten injunctions and civil penalties against banks that provide access to the payment system for certain merchants and third-party payment processors ("TPPPs") to whom they provide services. Without access to the banking and payments system, these entities are unlikely to be able to continue operating.[4] This was precisely the DOJ's goal from the outset.[5] Banks are disassociating with customers engaged in lawful behavior, not simply customers whose activities may be fraudulent, as bankers try to define the next targets of the DOJ's efforts. The DOJ even acknowledged the prospects for such parties' banking relationships to be collateral damage of the DOJ's initiative.[6]

With Operation Choke Point, the DOJ is starting from the premise that certain lines of business or industries are anathema and then working backward to try to find legal violations. Using Section 951 of FIRREA to implement Operation Choke Point, the Government can issue subpoenas, take depositions, and seek civil damages against entities committing mail or wire fraud "affecting a federally insured financial institution."[7] In doing so, the DOJ need only meet the lower, civil evidentiary burden of proof ("by a preponderance of the evidence") to demonstrate fraud.[8] The DOJ's objective, however, is not to bring any action against those suspected of committing fraud, but to cause a bank "to scrutinize their account relationships and, if warranted, to terminate fraud-tainted processors and merchants."[9] Over the bank's head, the

---

[1] Peter Weinstock is a partner in Hunton & Williams's Dallas office whose practice focuses on corporate and regulatory representation of financial institution franchises. This written statement presents the views of Mr. Weinstock and does not necessarily reflect those of Hunton & Williams or its clients. The information presented is for general information and education purposes. No legal advice is intended to be conveyed. Mr. Weinstock may be reached at (214) 468-3395 or pweinstock@hunton.com.

[2] DARRELL ISSA, THE DEPARTMENT OF JUSTICE'S "OPERATION CHOKE POINT": ILLEGALLY CHOKING OFF LEGITIMATE BUSINESSES? (U.S. House of Representatives Committee on Oversight and Government Reform, 2014) at 2 (citing Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney General, Office of Legis. Affairs, U.S. Dep't of Justice, to Rep. Blaine Luetkemeyer (Sept. 12, 2013) (stating "[t]he Department seeks to combat fraud and other unlawful practices in the payment system, and our efforts are focused on all those engaged in illegal activity."); Congressional staff briefing with the Deputy Assistant Attorney General for Consumer Protection, Civil Div., U.S. Dep't of Justice, on Sept. 20, 2013).

[3] Codified under 12 U.S.C.A. § 1833a.

[4] Issa at 1.

[5] *See generally* Nov. 5, 2012 Letter from Joel M. Sweet to Stuart F. Delery, Acting Assistant Attorney General (Civil Division) (HOGR-3PPP000020).

[6] *See, e.g.*, Nov. 5, 2012 Letter from Joel M. Sweet to Stuart F. Delery, Acting Assistant Attorney General (Civil Division), at 2-3 (HOGR-3PPP000020).

[7] *See* 12 U.S.C.A. § 1833a(a), (c).

[8] *See* Allyson Baker & Andrew Olmen, *FIRREA: The DOJ's Expansive (and Expensive) Tool of Choice*, 28 No. 10 Westlaw Journal Delaware Corporate at 1 (2013).

[9] *See, e.g.*, Nov. 5, 2012 Letter from Joel M. Sweet to Stuart F. Delery, Acting Assistant Attorney General (Civil Division), at 3 (HOGR-3PPP000020).

DOJ holds FIRREA's expansive reach, lower burden of proof, heavy monetary penalties, and ten-year statute of limitations.[10]

As a result of the DOJ's use of FIRREA, banks have been forced to choose between, at a minimum, incurring significant discovery and compliance costs and potentially accepting costly penalties, on one hand, or terminating existing relationships with TPPPs and other merchants that may be operating lawfully, on the other hand. The DOJ has calculated that banks' sensitivity to the costs of responding to the DOJ's inquiry, let alone to "civil/criminal liability and regulatory action," will cause a bank "to scrutinize immediately its relationships with [TPPPs] and fraudulent merchants and . . . take necessary action [*i.e.,* cut them off]."[11] In Operation Choke Point, the determination of whether a merchant is fraudulent is determined by the DOJ based on a line of business, rather than by an adjudication where those who are accused are afforded due process. The DOJ believes that "[l]egitimate banks will become aware of perhaps unrecognized risks and corrupt banks will be exposed."[12] In other words, a bank that does not agree with the DOJ's assessment, perhaps based only on return rates—which the DOJ concedes is only a "red flag of ***potential*** fraud"—will be deemed "corrupt" and subject to legal action.[13] Operation Choke Point has had a chilling effect on banks' ability to transact with such TPPPs and merchants where the reward cannot compensate for the potentially enormous costs and potential exposure under the DOJ's use of FIRREA. Banks are forced to drop these entities, but the affected TPPPs and merchants have no recourse to combat this penalty. It effectively becomes an extra-judicial permanent injunction by the agreement of government lawyers and an (appropriately) skittish bank.

In stating that its goal is to "positively sensitize the banking industry to third-party payment processor risk,"[14] the DOJ is launching an offensive against TPPPs and classically using enforcement to regulate, if not legislate away, organizations that may very well be legitimate. Such an approach is the province of rule-making under statutory authority with appropriate notice and opportunity to comment, and potentially, to challenge the adoption of the rule. This broad expansion of FIRREA triggers concerns that the DOJ has exceeded its authority under the statute or, if it has not done so, that the statute has no outer limit and is thus vague.

II. Flaws in the DOJ's Approach

FIRREA was passed in response to the Savings and Loan crisis of the late 1980s in part to curb "outright fraud and insider abuse" committed against depository institutions.[15] Through FIRREA, Congress aimed to protect depositors in financial institutions and federal taxpayers from fraudulent conduct that could result in a taxpayer-funded bailout.[16] With the federal government's current analysis, that intent is turned on its head. Instead of using FIRREA to protect banks from fraud, the DOJ is prosecuting banks for conducting disfavored business and then using discovery, including a draconian subpoena power, to try to find activity that can be

[10] 12 U.S.C.A. § 1833a(h).

[11] Nov. 5, 2012 Letter from Joel M. Sweet to Stuart F. Delery, Acting Assistant Attorney General (Civil Division), at 2-3 (HOGR-3PPP000020).

[12] *Id.* at 3.

[13] *Id.* at 2-3 (emphasis added).

[14] *Id.* at 3.

[15] *See* Issa at 3.

[16] *Id.* at 455.

deemed illegal. Entities shut out of one bank have little hope of establishing a subsequent banking relationship and will become defunct without any opportunity to defend themselves. While I am not championing the efficacy of payday lending, there are undoubtedly some organizations that operate lawfully and provide unbanked customers with a service such customers believe is valuable, one less dangerous than engaging a loan shark.

Indeed, a review of the development of Operation Choke Point reveals this new technique. As noted by the House Committee on Oversight and Government Reform, "internal memoranda on Operation Choke Point clearly demonstrate that the [DOJ's] primary target is the short-term lending industry. . . ."[17] Brandishing FIRREA as a sword, the DOJ chose to go after a number of banks that were doing business with TPPPs to get them to cease providing services to these entities. There was no proof when such decision was made that any of these banks were affected by fraud. Instead, in designing Operation Choke Point, the DOJ stunningly proposed identifying ten "suspect" banks for analyzing return rate data, among other "criteria."[18] However, the DOJ's "standards" for identifying fraudulent activities were arbitrary and relied almost exclusively on NACHA average return rate instead of potential violations of state—not federal—consumer protection laws.

NACHA is a private trade organization that administers and facilitates private-sector operating rules for ACH payments, which define the roles and responsibilities of financial institutions and other ACH Network participants.[19] The DOJ has alleged that an overall return rate of 3% on all of a merchant's ACH transactions should be the benchmark for what is considered fraud, because it is higher than the industry average tracked by NACHA. This is misleading. The overall return rate does not distinguish among the type of the return (unauthorized entries are very different from returns due to insufficient funds) or the nature of the transaction or customer base. Thus, the DOJ is not distinguishing between unauthorized return rates and returns due to insufficient funds. Furthermore, the DOJ compares the card networks' rate of disputed transactions to the overall ACH return rates, even though those are two completely disparate numbers. Card network disputed rates do not include transactions that are declined when the card is swiped. ACH returns, on the other hand, can include cases of insufficient funds or incorrect account information, along with debits disputed by the accountholder. The test employed by the DOJ to catch fraud may have resulted in legal businesses being considered fraudulent, too. It certainly resulted in dozens of banks and TPPPs receiving subpoenas. Accordingly, under the standards the DOJ is promulgating, it may advise a bank that a TPPP is engaged in fraud, ignoring legitimate reasons for a relatively high return rate, and expect the bank to terminate the relationship or incur significant discovery costs.

The DOJ has not commented on why it failed to take into account the long-standing relationships between the banks and the TPPPs, the previous reviews of the banks and TPPPs conducted by examiners, and the Treasury Department determination that TPPPs are not money transmitters and are not required to register with FinCEN. The DOJ's proposed use of mathematical proxies to allege fraud is a frightening prospect and far afield from what most federal prosecutors do

---

[17] Issa at 5.

[18] *See* Nov. 5, 2012 Letter from Joel M. Sweet to Stuart F. Delery, Acting Assistant Attorney General (Civil Division), at 4 (HOGR-3PPP000020).

[19] *See About NACHA*, accessible at https://www.nacha.org/about.

before bringing a fraud case. This type of activity has the potential to erode confidence in the DOJ.

The "chilling effect" of Operation Choke Point is not limited to the DOJ's actions. Instead, it is partially predicated on the notion that "reputational risk" arises when banks transact with TPPPs and certain "high-risk" merchants.[20] What constitutes "reputational risk," however, is not clearly defined. The Federal Deposit Insurance Corporation ("FDIC") issued a Financial Institution Letter entitled "Guidance for Managing Third Party Risk" that explains reputation risk as "the risk arising from negative public opinion" and adds "any negative publicity involving the third party, whether or not the publicity is related to the institution's use of the third party, could result in reputation risk."[21] Federal Reserve Board Governor Sarah Raskin explained "reputational risk" in a speech by stating that "enterprise value comes from intangible assets such as brand recognition and customer loyalty that may not appear on the balance sheet but are nevertheless critical to the bank's success."[22] Raskin further added that supervision of banks is necessary in order to prevent the accumulation of reputational risk to the extent that it constitutes a hidden exposure.[23] These comments illuminate the vague and subjective standard now being wielded by the federal government against banks doing business with disfavored industries. The "guidance" plainly does not distinguish between lawful and fraudulent activity. Reputational risk is not legal risk. Regulatory authorities proffer no standard of how to evaluate whether, as Raskin states it, that reputation risk is "accumulating" and that any "exposure" is material to safety and soundness.

Moreover, the Office of the Comptroller of the Currency and the Board of Governors of the Federal Reserve System issued guidance in the fourth quarter of 2013 emphasizing the need for bankers to risk assess their customer base.[24] High-risk businesses require more extensive oversight, including potentially third-party testing of such parties' compliance management systems ("CMS"). To further define such businesses that may give rise to reputational risk, the FDIC published an article on its website.[25] This article sets forth 30 merchant categories that are deemed to be "high risk" in nature. Examiners, and thus bankers, are using this list as a touchstone informing what business relationships are disfavored. However, the list of merchant categories included seems somewhat arbitrary. Other merchant categories possibly could present higher risk to banks, but are not included. Examples of potentially high risk businesses not included on the FDIC's list include phone companies, financial advisors, personal trainers and tax preparation firms. Nevertheless, bankers have been relying on the FDIC list when determining with which firms to transact business.

---

[20] *See* Issa at 1.

[21] *See* "Guidance for Managing Third Party Risk." FDIC, Financial Institution Letter: Guidance for Managing Third Party Risk, FIL-44-2008 (June 6, 2008).

[22] *See* Sarah Bloom Raskin, Federal Reserve Board Governor, Address to the 2013 Banking Outlook Conference at the Federal Reserve Bank of Atlanta (Feb. 28, 2013).

[23] *See id.*

[24] *See* "Guidance on Managing Outsourcing Risk." Board of Governors of the Federal Reserve System, SR 13-19/CA 13-21 (Dec. 5, 2013); "Risk Management Guidance." OCC Bulletin 2013-29 (Oct. 30, 2013).

[25] *See* FDIC Supervisory Insights – Summer 2011, *Managing Risks in Third-Party Payment Processor Relationships*, accessible at http://www.fdic.gov/regulations/examinations/supervisory/insights/sisum11/managing.html.

All of the guidance and the article regarding the "reputational risk" standard and high risk enterprises were promulgated without the requisite notice and comment period and without any administrative record. The nature of this new approach to knowing your customer goes well beyond the mandates of the Bank Secrecy Act and the Anti-Money Laundering laws and the US PATRIOT Act. While those statutes focus on potential money laundering and financial fraud, the new focus is potentially much broader, requiring banks to police their customers' CMS.

III. Effects of the DOJ's Overreach

With the expansion of Operation Choke Point, many banks simply are ceasing to provide services to TPPPs or high-risk merchants. The result is that TPPPs and other merchants labeled "high risk" no longer have access to deposit systems from regulated financial institutions. Without this access, these businesses may be forced to shut down.[26] Small and mid-size businesses who use TPPPs will no longer have an economical option for processing payments. These businesses rely upon TPPPs, because costs are prohibitively high to establish electronic systems to access the banking system and go through a bank directly. In fact, the vast majority of payroll in this country and the tax payments for payroll are performed by TPPPs. Shutting down TPPPs will upend this method of doing business. Currently, TPPPs and their merchant customers are looking to adopt bank-like levels of CMS. The costs of such compliance must be paid. In short, among other flaws, Operation Choke Point threatens electronic access to the banking system or risks imposing costs on small businesses, both of which are crucial components of the economy.

IV. Conclusion

Operation Choke Point represents a fundamental shift in law enforcement and regulation. The DOJ is using an obscure section of FIRREA intended to address those who caused losses to savings associations to justify imposing legal and regulatory pressure on banks serving disfavored businesses. As a result of Operation Choke Point, banks are forced to deny services to these disfavored entities or risk heavy civil penalties, criminal liability or regulatory action, even without any evidence that the banks have done anything wrong. TPPPs, in particular, have been targeted by the DOJ through these "back door" means. The DOJ is accomplishing its goal, but at what costs to the business community and consumers?

[26] If they seek to survive, these entities must turn to non-traditional sources of credit, which come with a very high risk and little regulation.

Mr. BACHUS. Mr. Holding, recognized for questions.

Mr. HOLDING. Thank you, Mr. Chairman.

Mr. Thompson, thank you for your testimony.

There is a little bit of a discrepancy amongst the panel here. In his testimony, Professor Levitin states that there are no verified cases of banks terminating accounts in direct reaction to Operation Choke Point.

I heard you testify differently than that. So, if you could, please explain where that discrepancy comes from.

Mr. THOMPSON. Sure. And perhaps it is definitional in terms of what we mean by Operation Choke Point. But what I mean by that is the coordinated effort by the Department of Justice, the FDIC, the OCC, and the Fed to target certain high-risk industries.

And this is what we saw in that subpoena and the attachment to the subpoena. And if that is what we mean by it, we have heard numerous instances of banks saying, "We are getting out of"—"We are exiting this relationship," relationships that often extend over a decade, almost 2 decades.

And there has been no indication that there was a concern about the risk profile, that anything had changed in the risk profile of the short-term credit lender. Rather, it was regulatory pressure. That is what we are hearing, regulatory pressure, and it is clear that it is Operation Choke Point.

Mr. HOLDING. And you are in the business of representing similarly situated entities on a daily basis. Correct?

Mr. THOMPSON. Yes. That is right.

Mr. HOLDING. The—you know, talking about these subpoenas, again drawing on your experience as a practicing attorney in this field, the—take a minute and walk through, you know, what happens when a client gets a subpoena like this. You know, what is the ripple effect? And, ultimately, at the end of day, you know, what does it cost them to respond?

Mr. THOMPSON. Well, it is a very significant cost in any number of respects. It starts with just answering the subpoena, which means retaining lawyers, number one.

Number two, typically, then these subpoenas are looking for emails. The cost of production can be hundreds of thousands of dollars just in computer resources to do an email sweep and then to produce, depending upon the volume of material that is sought.

And often, of course, the subpoena is a prelude to further investigation, which would cost—could cost millions of dollars. And then you layer on top of that the bad publicity that comes from receiving this, the investigation.

There is enormous pressure on the institution to make it—the pain stop. And I suspect, although I don't know, that that is one of the reasons we see 50 subpoenas being issued, but only one case being—having to be filed, because there is huge asymmetric pressure when the government issues a subpoena on a recipient to try to make the pain stop.

Mr. HOLDING. So if you are a financial institution, I mean, you are always looking at the bottom line, doing a cost-benefit analysis. Whether you take on a client or retain a client, you know, you certainly do a risk analysis as to whether they will be able to repay their loans, whether they will be a profitable customer.

But then you add into that—you know, if they fall into one of these high-risk categories, as enumerated by the FDIC, the—you look at that and say, "You know, it could cost me a lot of money to have this person as a client." Correct?

Mr. THOMPSON. You are absolutely right.

And it is not limited just to that. Because, as one of the panelists—or Members of the Subcommittee indicated earlier, regulators have a lot of different ways to apply pressure on a financial institution.

So, yes, you are right. The dollars and cents are huge. The negative publicity is very significant. But, also, you want to try to stay on the right side of your regulators. And if you defy them, they have innumerable ways to get even with you.

Mr. HOLDING. Thank you.

Mr. Chairman, I yield back, in light of the vote.

Mr. BACHUS. Thank you. I appreciate that, Mr. Holding.

Do you want to go ahead and begin to ask one or two questions and then we will break in maybe 2 minutes? We have 3 minutes left on the floor. Or do you want to come back?

We will wait.

We would like to come back. Are any of you all under a time restraint?

All right. We will—there are two votes on the floor?

Mr. JOHNSON. That means everybody is on the clock?

Mr. BACHUS. I think that may be probably 30 minutes. Why don't we do this. Why don't we come back at 10 till. Is that all right? Or 15 till? That will give you a chance to get something to eat. We are going to come back at 15 till. Probably won't come back. Let's say 20 minutes. 20 minutes.

Mr. WEINSTOCK. How long do you think we will go from there, Mr. Chairman?

Mr. BACHUS. 20 minutes max. We will be out of here by 1:00, 1:15.

Mr. WEINSTOCK. Thank you.

Mr. BACHUS. Is that okay?

Mr. WEINSTOCK. I am not on the clock.

Mr. BACHUS. Oh, no. Okay. So you are not getting paid right now.

Mr. WEINSTOCK. I am here of my own volition.

Mr. BACHUS. We will try to get you out of here pretty quick.

Mr. WEINSTOCK. Thank you, Mr. Chairman.

Mr. BACHUS. Of course, a professor gets paid by teaching classes. So he is a little better——

We will recess at this point.

[Recess.]

Mr. BACHUS. The Subcommittee will come to order.

My first question will be for Mr. Weinstock.

Mr. WEINSTOCK. Yes, sir.

Mr. BACHUS. Well, actually, no. That question has been asked. So George asked that question. I just saw where I marked it off.

Mr. Talbott, people might be skeptical of the idea of an industry policing itself. Are there any economic incentives that explain why one could expect that the payment industry would do a good job of fighting fraud?

Mr. TALBOTT. Sure. Thank you, Mr. Chairman. Appreciate the question.

Because fraud, in case of credit card or debit card, that is visited upon the consumer comes bank to not the consumer—the network rules prohibit banks or processors from charging the customer—because that fraud comes back to the payments industry, we have to bear the cost of that fraud.

We have a direct pecuniary interest ensuring that fraud is kept off the system. So in addition to it being good public policy, it is—comes directly out of our bottom line. So we have every incentive to ensure that fraud stays off the system.

Mr. BACHUS. All right. Thank you.

Mr. WEINSTOCK. Mr. Chairman, can I add a comment?

Mr. BACHUS. Yes.

Mr. WEINSTOCK. One thing people don't realize is NACHA applies fines very quickly if there are unauthorized transactions and the bank can't show proof that the customer authorized the transaction.

After three, four instances, that equals a fine of over six figures. So it is not like it is a toothless exercise. If they don't pay the fines, they can get kicked out NACHA.

Mr. BACHUS. Okay. Thank you.

Mr. LEVITIN. Mr. Chairman, if I may add, I agree with all of that. But I think it is important to note that it is—only part, not all, of fraud costs come back to industry.

Because what it—you don't have perfect enforcement going on because a lot of consumers will just lump it on a small-dollar fraud. It is not worth complaining about $10 or $20 that are wrongfully debited.

So when consumers complain, yes, the industry is at risk, but consumers often don't complain about small-dollar frauds.

Mr. BACHUS. Professor, same point that we are discussing. You did—I think in your testimony you were the one that covered the fact that—you said a payday lender is out of business if he—out of business or insolvent, the payday lender's bank bears the loss, and that that is one reason—justification, you know, for——

Mr. LEVITIN. That's correct.

Mr. BACHUS. They can—but let me ask you this. You then went on and said banks already charge those merchants much higher fees for banking service precisely because of the risks they pose, over on page 11.

So you—you know, you say that there is some risk, but then in another paragraph, you acknowledge that a bank can just set a higher fee. And you mention that there are a lot of businesses that just have higher return rates, I mean, as a—as a matter of just their business. So——

Mr. LEVITIN. Sure. Return rates do vary by industry. And it is important that we distinguish between absolute return rates and return rates because of unauthorized transactions. Not every return—ACH return is because of an unauthorized transaction.

Mr. BACHUS. Yeah. And I agree with that. But, still, banks have an ability to adjust.

Mr. LEVITIN. Oh, I agree completely, Mr. Chairman, and that is actually, I think, the important point, which is that, if Operation

Choke Point is imposing higher costs on high-risk merchants, there will be some banks—we have got almost 7,000 banks in the United States; it is far more than any other country has—there will be some banks that see this as a business opportunity and say, "Hey, archery store that got closed down, come to us. We are going to charge you more, but we will take your business. We will do the diligence on you. We can get comfortable with you. It is going to just cost you more."

And the market should correct this. You know, it may not be a perfect correction, but we should see a market correction.

Mr. BACHUS. Let me say this to you. You know, I know—I notice that you—and you are the witness that was called by the—by the Democratic party, you know—I mean, Democratic colleague. You actually talked about two or three times that justification for this is anti-money laundering.

Mr. LEVITIN. I am sorry, Mr. Chairman. I didn't understand.

Mr. BACHUS. You said—you, you know, criticized our attempts to hamper the Justice Department's enforcement of anti-money laundering law and, you know, you actually say that is what they are trying to do, prevent anti-money laundering.

Because that is the justification for this program. Right?

Mr. LEVITIN. I think that is correct, sir. Operation Choke Point, if you look at the actual complaint, that is the—you know, the—the—it—the problem that was alleged with Four Oaks Bank was a failure to essentially know your customer. With the Bank Secrecy Act anti-money laundering——

Mr. BACHUS. And that has to do with money laundering.

Mr. LEVITIN. That is right. And it is important to recognize that, when you have an anti-money laundering problem, even if it is from, let's say, a payday lender, that can actually implicate much broader things because, if a bank doesn't know its customer, it doesn't actually know what that transaction is.

Just because a business says it is a payday lender, it can also be, you know, engaged in other business, allowing other transactions to be routed and look like they are payday loans.

Mr. BACHUS. Right. Yeah. And, you know—and I mention this because that is an argument that we are hearing from some of our colleagues.

You know, you say Operation Choke Point is ultimately an anti-money laundering enforcement that requires the banks to take their know-your-customer duties seriously.

And that is—the Justice Department, you know, on one hand, has said it is for this reason, but then they said, well, actually, it is to prevent money laundering.

But do—do payday lenders launder a lot of money? Is there any evidence of that?

Mr. LEVITIN. As to actual money laundering, I don't know of any evidence on that. We do know that there is high return rates, however.

Mr. BACHUS. Well, yeah. But I am talking about—you know, I am talking about money——

Mr. LEVITIN. And—well, I think it is important that we define what we are talking about with money laundering. Money laun-

dering is not limited to narcotics or terrorism. Money laundering is just proceeds of any illegal transaction.

Mr. BACHUS. Yeah. Right.

Mr. LEVITIN. And to the extent that you have illegal transactions going on in any industry, payday loans or what have you, then, yes, there can be a money laundering problem.

Mr. BACHUS. Are these hundred-dollar loans? But you said there is no evidence that the——

Mr. LEVITIN. I don't know of any evidence. I have never investigated this.

Mr. BACHUS. Yeah. Right. Okay.

Mr. LEVITIN. I would note, though——

Mr. BACHUS. I am sure potential is there for any——

Mr. LEVITIN. Of—sure.

Mr. BACHUS [continuing]. By any industry. I mean, you know, in fact, people buy cars. One of the primary ways is they go to a car dealership. They buy a very expensive car. Then they turn around and they sell it. And they deposit the proceeds and they launder it that way. But, you know, car dealerships are——

Mr. LEVITIN. There is a particular concern, though, in that some payday lenders are also money services businesses and they are sometimes engaged in doing international remittances. And that raises particular money laundering concerns.

Mr. BACHUS. I think the—you know, if you are talking about a hundred dollars at a time, it is kind of hard to——

Mr. LEVITIN. Well, that—but that is the way to do money laundering. It is called smurfing.

Mr. BACHUS. No. No. Actually——

Mr. LEVITIN. You do it in small transactions so you don't get——

Mr. BACHUS. You know, cars are a $10,000 transaction, I think. Money laundering, through—you know, when they do drugs to money, they are converting—they are not doing it a hundred dollars——

Mr. LEVITIN. Actually, I disagree with you on that, sir, because banks have—have to file suspicious activity reports for anything over $10,000.

The idea is you keep your—if you want to be a money launderer, you keep your transactions small and you don't put them at 9,999 because that is also suspicious. You make smaller transactions, not necessarily a hundred.

Mr. BACHUS. No. No. I——

Mr. LEVITIN. But you break it up into little pieces——

Mr. BACHUS. Maybe 2,000, 3,000. Or you buy—you know, there are—people buy appliances and they ship them back—out of the country. You know, there is a lot of that.

But I have seen no—I mean—I have never seen any evidence that people are cashing their paychecks—I mean, a paycheck is a—that is a—that is not cash.

They are actually taking a check. And there is no need to money-launder that. And they are turning it into cash. They are not turning cash into a check.

So—but, anyway, I—we are—I have done 7 minutes. We will—my colleague will do 7. And then we will turn—I just was pointing out——

Mr. JOHNSON. Okay. Thank you.

Professor, you are a professor. And you three gentlemen, Mr. Talbott, Mr. Thompson, and Mr. Weinstock, are practicing lawyers. Is that correct?

Mr. TALBOTT. Yes.

Mr. THOMPSON. Yes.

Mr. TALBOTT. I am a lobbyist——

Mr. JOHNSON. You are a lobbyist.

Mr. TALBOTT [continuing]. With a law degree.

Mr. BACHUS. He is government affairs.

Mr. TALBOTT. I am not apologetic.

Mr. BACHUS. You are government affairs.

Mr. JOHNSON. The three of you also have clients; do you not?

Mr. THOMPSON. Yes. Yes, sir.

Mr. BACHUS. And, Mr. Thompson with Hunton & Williams—oh. I am sorry.

Mr. Weinstock with Hunton & Williams, you have many clients in the financial services industry; do you not?

Mr. WEINSTOCK. Yes.

Mr. BACHUS. And how about you, Mr. Thompson?

Mr. THOMPSON. I do not. In the past, I have represented, but not at present. I have some.

Mr. JOHNSON. And Mr. Talbott?

Mr. TALBOTT. Members of the association of ETA are payment companies. Some are financial institutions, per se. Others are not.

Mr. JOHNSON. Okay. And—but, now, Mr. Thompson, you have done over 50 depositions. Did I hear that earlier?

Mr. THOMPSON. I think it is several hundred, in fact. But only two of Members of Congress, Senator Snowe and Representative Meehan back in the McCain-Feingold case.

Mr. JOHNSON. Okay. And you did that work in connection with your job responsibilities where?

Mr. THOMPSON. At Cooper & Kirk. I have been there since 1996.

Mr. JOHNSON. And so that law firm does represent clients in the financial services industry?

Mr. THOMPSON. We have. Yes.

Mr. JOHNSON. And so—and I—and I suppose, in a perfect world, a perfect corporate world, a perfect free market corporate world, a perfect free market Ayn Rand-style world, there be no regulations on banks at all.

Would you agree with me on that, Mr. Talbott?

Mr. TALBOTT. Theoretically, if you asked Ayn Rand, I think she would answer that question in the positive.

Mr. JOHNSON. Well, how about you?

Mr. TALBOTT. I think that there is a need in—for some regulations some places, financial services probably less so than other areas. But there is a value to having some regulations.

Mr. JOHNSON. Mr. Thompson?

Mr. THOMPSON. My clients are not contesting the validity of any of the regulations or——

Mr. JOHNSON. No. My question is: Would you agree that that would be a perfect world for corporations, to not have any rules or regulations——

Mr. THOMPSON. No.

Mr. JOHNSON [continuing]. And they could pretty much self-regulate?

Mr. THOMPSON. No, Congressman. That——

Mr. JOHNSON. Is that the kind of world that we want, Mr. Weinstock?

Mr. WEINSTOCK. I never read the book. So I am not exactly sure why a Rand-perfect world would be. But I think what we are all saying is what is appropriate is balance in regulation.

Mr. JOHNSON. Well, now, how can we have reasonable regulations if the banking institutions don't want to deal with the potential loss of customers because they determine for themselves that their reputational risks—that the reputational risks are not worth the business and you have to also do more oversight, got to do more—the costs of doing business for certain businesses is high because of regulation, and you would prefer to not have to—for your clients to not have to incur those costs. And I understand that.

But where do we draw the line? Where is regulation meaningful and reasonable and in the public interest?

And so that is a fundamental question I think we have to deal with as opposed to an incendiary guilty-until-proven-innocent study of propriety and legal authority for the Justice Department's Operation Choke Point.

I mean, Operation Choke Point has only resulted in one civil action. Subpoenas have been sent out to other institutions. There are ongoing investigations.

But a settlement in a civil case—and we are sitting up here wasting, you know, your time bemoaning the fact that your clients have to incur costs of doing business.

I mean, you know, when is the—when do we—who protects the consumer, which is the real customer?

Mr. WEINSTOCK. Can I respond?

Mr. JOHNSON. Yes.

Mr. WEINSTOCK. In terms of the level of regulation, as they say in East Texas, if you hang the meat too high, the dogs won't jump.

And the problem for our client base, which they are community banks, they are the lifeblood of their local communities, is that, if the level of regulation is such that they have a duty to police all of their customers, their scripts——

Mr. JOHNSON. Well, shouldn't that be just a normal cost of business, that you do your due diligence and you make sure that certain benchmarks are met with enhanced scrutiny, like rate of returns in excess of 1.5 percent?

Isn't it—I mean, isn't that the regulations of your industry, Mr. Talbott?

Mr. TALBOTT. Yes.

Mr. JOHNSON. And so, if—if regulators or the Department of Justice notes some benchmarks that have been met which trigger suspicion, you all seem to be opposed to DOJ following up on that. You just want there to not be a loss of the customer——

Mr. WEINSTOCK. That is not what we are saying, Congressman.

Mr. JOHNSON [continuing]. And you don't want a loss of the cost of doing business, and it just seems very Utopian to me.

Mr. WEINSTOCK. If—in terms of the 1½ percent, that is really a red hearing. That is an average based on lots of different NACHA

transactions. The DOJ disowned the 3 percent, which was just mathematically doubling the 1½ percent average.

NACHA, which is the agency that calculates the averages, never indicated that it is an indicator of fraud. The DOJ took it on itself and then at this hearing disowned the 3 percent.

Unquestionably, banks have an obligation to know their customer. Banks are complying with that obligation to know the customer.

Where this is all insidious is if the level of regulation and the level of supervision is such where the bankers don't believe they can ever chin the bar, they can ever jump and catch the meat.

Then their smart thing to do is to de-risk, cut the customer off. And the costs we are talking about are access to the lifeblood of an electronic economy.

Mr. JOHNSON. Yeah. Well——

Mr. BACHUS. Actually, we did 7 minutes. So it is 8½. You can go ahead, if you have got another question, and then I will——

Mr. JOHNSON. I just wanted to ask Professor Levitin did he have anything he wanted to say in response to what we have heard.

Mr. LEVITIN. Again, I would just say that I am not sure that—I am not sure I would agree with Mr. Weinstock.

Certainly for some banks they will decide that it is not worthwhile serving high-risk customers. They just can't get—that they are afraid that their compliance costs are just going to be too high to get comfortable with it.

But we have nearly 7,000 banks. Unless we assume that we have a real market failure in the banking industry in this particular area, there will be banks that will step up and serve these high-risk clients.

They will start specializing in it. They are going to do more diligence. It will cost them more. It will cost the clients more. It will cost Mr.—and high-risk businesses will have to pay more for access to the banking system.

But that is exactly the way it should be. Parties should bear their own risk. If you are imposing costs on the system, you should have to internalize them. And I don't think there is anything wrong with that.

Mr. JOHNSON. Well, I think that would be the way that Ayn Rand would want it to be.

Mr. LEVITIN. I would just add it is not clear to me that markets exist except with regulation. If you try and imagine a totally unregulated market, I think that looks like the Mogadishu arms bazaar, and I don't think that is the way we want our economy to operate.

Mr. BACHUS. Let me start with that. I somewhat—I agree with you. I think that the market needs to be regulated.

That is really why I am just, you know, disturbed about payday lenders, short-term lenders, being put out of business. Let me explain why. And I think history is a good teacher.

Mr. Johnson talks about a perfect world. In a perfect world, there will be no payday lenders. But there always have been. In the South, do you know who the payday lender was in many cases?

Mr. LEVITIN. It was often the employer.

Mr. BACHUS. It was—no. It was—there were some—some occasions where the employer—you are absolutely right. You had the company store where people bought things——

Mr. LEVITIN. I was thinking of Faulkner, actually. He has got Old Man Snopes loaning sawmill workers a dime on Sunday. And they are supposed to pay it back with a penny the next week.

Mr. BACHUS. That is right.

Mr. LEVITIN. Never asked for the dime back. Just keeps taking a penny every week.

Mr. BACHUS. And I actually had two employers and they—many times was a high interest rate. They don't loan money anymore. I mean, I don't know of any—very few cases. You don't have a lot of company stores.

What you do have is you have the sheriff in those counties or you have a guy that is just a self-appointed guy that stands outside the—used to stand outside the gate when people got their paycheck. You know, he—or—you know, he—he was waiting to get his money back. During the week, he had loaned at a 50 percent or a 30 percent.

A lot of times, though, it was—it was totally unregulated. And people got their arms broken. People got their fingers mashed. People got beat up. So we—States wanted it regulated, and they set rules. And that is the rules we have today.

So these payday lenders are—you know, if you—if they go out of business, you are going to have the guy at the gate getting his money back. And if he doesn't get his money back, kind of like in the—gambling used to be. You know, when you have unregulated gambling, people get—people get hurt, people get killed.

So, really, you shut these down, you are going to have people loaning money. And they are going to be unregulated. They are not going to answer to anybody. So this isn't about regulation. It will be Mogadishu again, like you said, I mean, about something else.

I just say consider that. And you talk to anyone that ran a plant in the South, they will tell you there was always a payday lender. And—you know, and a lot of times you share for the probate judge.

That is how they made their money. There were other things that—they used to make their money on illegal whiskey by protecting some people. They were in the protection business.

Mr. LEVITIN. Mr. Chairman, I think it is important to note that payday loans basically don't make money absent customers get stuck in a—in a debt trap.

Let me illustrate. Online payday lenders buy leads. If you go to a Web site looking for a payday loan, that is actually a lead-generator's Web site——

Mr. BACHUS. No. I understand.

Mr. LEVITIN [continuing]. Get auctioned off.

Mr. BACHUS. Professor, what I am saying, you know, you—in a perfect world, I would never argue with you that, you know, it—but I would tell you there will always be a payday lender, and it will be unregulated or regulated. Those are our two choices.

You know, one thing you do is you talk about Congress should not be using its oversight power to subsidize these businesses. You say that twice.

Mr. LEVITIN. That is correct.

Mr. BACHUS. And you say payday lenders, online gun shops, escort services, online gambling parlors—now, they are all illegal. That is flat out prohibited.

Mr. LEVITIN. Actually, I am not sure that any of those are, per se, illegal. There is a small sliver of online gambling——

Mr. BACHUS. Yeah. The wire——

Mr. LEVITIN. Similarly, escort services, if they are very narrowly only companionship——

Mr. BACHUS. Yeah. But I will just say most of your gambling online. You know, it is hard to stop. A lot of them are overseas. But purveyors of drug paraphernalia and racist material, pornographers that serve no clear public service.

But, you know, you—when you get into saying that, you are equating short-term lenders. I mean, you are making a judgment there that—you are equating them to drug purveyors or drug paraphernalia. I know you don't intend do that.

Mr. LEVITIN. No. No. No. Actually, I think for——

Mr. BACHUS. Or online gun shops.

Mr. LEVITIN [continuing]. For the purposes of what I am saying, I very much intend—intend that because——

Mr. BACHUS. Okay.

Mr. LEVITIN [continuing]. In terms of whether these are high-risk merchants or not, from a bank's perspective, it doesn't really matter what the ultimate transaction is. It is how much risk.

And the porn Web site and the payday lender, if they are high risk, they are high risk. It doesn't—the specifics of the industry don't matter. It is high risk.

Mr. BACHUS. But, you know, I think—when you are talking about a criminal investigation by the Justice Department, I think it matters whether it is a legitimate business or a fraudulent business. That is my point.

Mr. Thompson, FIRREA passed in 1989. It was never used until now against payment processors, was it?

Mr. THOMPSON. Mr. Chairman, I am not an expert on that aspect of FIRREA, but I believe you are correct.

Mr. BACHUS. Yeah.

Mr. Talbott, do you know.

Mr. TALBOTT. Same answer. I think that is right.

Mr. BACHUS. Okay. I think that concludes our hearing today. I appreciate all our witnesses. Concludes the hearing.

Did you have another question.

Mr. JOHNSON. No, sir. I do not, Mr. Chairman.

I just want to, for the record, thank the Chairman for his willingness to have these kinds of hearings that are not so structured and that—it prevents us from getting down into the meat of the matter. And so I want to thank you for——

Mr. BACHUS. Well, as you know, I am retiring after 22 years and I was a trial lawyer before I got here. And I don't think I could have ever tried a case on a 5-minute rule or even made a point, and it—the structure doesn't really lend itself.

And not in this particular hearing, but in some hearings it causes the witness to filibuster by talking about anything but answering the questions. But then it also—because Members rush

and I—I really hate to see Members do this, but they interrupt witnesses.

If the witness wants to give a 2-minute response, they want a "yes" or "no" answer. And that is not always possible. You want to explain yourself.

So you get—you really don't get a complete picture. You don't—you don't get—and then you have another witness wants to come in on what this witness said, which is good.

But we—so the 5-minute rule I wish we would—would do something about that in certain cases. But I am sure a freshman sitting down here wouldn't want that. But we could always start at the bottom every other time.

This concludes today's hearing. As I said, thank you for all our witnesses.

Without objection, all Members will have 5 legislative days to submit additional written questions for witnesses or additional materials for the record.

This hearing is adjourned.

[Whereupon, at 1:18 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

Statement for the Record
On behalf of the
Virginia Bankers Association
before the
House Judiciary Committee
Subcommittee on Regulatory Reform, Commercial and Antitrust Law
of the
U.S. House of Representatives

July 17, 2014

VIRGINIA BANKERS ASSOCIATION

Chairman Bachus, Ranking Member Johnson, and members of the subcommittee, VBA appreciates the opportunity to submit for the record comments regarding the Department of Justice's Operation Choke Point. The VBA represents all banks in the Commonwealth of Virginia and works collaboratively with the American Bankers Association on industry legislative issues.

This Subcommittee has continually sought the input of the financial services industry relative to the impact of the changing regulatory scheme on individual institutions' ability to serve their customers. We appreciate House Judiciary Committee Chairman Goodlatte's continued outreach and ongoing efforts to bring commonsense to the regulatory environment. The enormous challenges facing banks of all sizes, especially regional and community banks, in the face of the regulatory overreach contained in the Dodd-Frank Act cannot be understated. Cumulatively, the burden placed on banks attributable to the cost and complexity of compliance with the avalanche of new rules, regulations, guidance and supervisory decrees continues to produce unintended consequences on the fundamental business of banking. Ultimately, Virginians – including families, small businesses, and farmers – bear greater costs, less access to credit and fewer opportunities for investment in the communities our members serve.

Even by itself, the fallout of this regulatory overreach in recent years is troublesome as tax-paying Virginia banks seek to remain key partners to help achieve economic growth and job creation nationally and in our Commonwealth. While many institutions have and will continue to adjust to these significant changes and continue meeting the needs of their customers, additional obstacles only exacerbate the challenge. That is why the Department of Justice's initiation of

Operation Choke Point poses a wider concern than its individual effects, of which there are many.

Virginia banks have a constructive partnership with our state and national law enforcement agencies, built on a mutual desire to maintain integrity and security within our financial systems. The safety and soundness of that system is of critical importance to banks, their prudential regulators and law-abiding customers. Banks have a tremendous amount of responsibility to combat financial crime. Through compliance with the Bank Secrecy Act and Anti-Money Laundering statutes, banks make significant personnel and technology investments to carry out their unfunded role in assisting law enforcement. Unfortunately, that role continues to expand with greater complexity as banks are saddled with increasingly burdensome risk and responsibility beyond the traditional balance.

By initiating Operation Choke Point, the Department of Justice, in concert with some federal regulators, goes far beyond the bounds of that partnership. Pressuring banks to close accounts or sever services for targeted merchants deemed "high risk" by regulators, the Department has embarked on a disconcerting endeavor that undermines financial institutions' traditional role based on questionable legal authority. Extracting these demands through the threat of vicarious liability for bank customers' or customers' customers' activities, often without a court order or appropriate legal proceedings, is a misguided approach with serious consequences.

As Virginia banks face mounting compliance pressures, including within BSA/AML responsibilities, Operation Choke Point serves to further increase the operating and compliance expenses associated with the risk these undue pressures

some banks will be forced to make the unfortunate decision, in assessing the risk arising from the Department of Justice's inappropriate actions, to cease operations with legally licensed businesses. Law enforcement is best positioned to prosecute illegal behavior; forcing banks to discern and arbitrate what Justice has divined as their standard of conduct for legal business is not legal or effective.

Virginia banks will continue to partner with federal and state law enforcement to combat financial crime. However, Operation Choke Point should not be part of that partnership. We encourage a prompt and definitive end to Operation Choke Point, so banks, regulators and law enforcement can resume a balanced approach, with each contributing in a manner befitting their unique position in our financial system. We appreciate the attention of this subcommittee and other legislative bodies to this troubling initiative and support the legislative efforts to cease its continuation should Justice fail to terminate it of its own accord.

CFSA℠
COMMUNITY FINANCIAL SERVICES ASSOCIATION OF AMERICA
A COMMUNITY OF RESPONSIBLE LENDERS

515 KING ST., SUITE 300
ALEXANDRIA, VA 22314-3137
PHONE 888.572.9329
FAX 703.684.1219
E-MAIL INFO@CFSAA.COM
ONLINE WWW.CFSAA.COM

Community Financial Services Association of America
Statement for the Record

House of Representatives Judiciary Committee
Subcommittee on Regulatory Reform, Commercial and Antitrust Law

"Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke"

July 17, 2014

I. Overview

The Community Financial Services Association of America ("CFSA")[1] appreciates the opportunity to provide comments on the House Judiciary Committee's Subcommittee on Regulatory Reform, Commercial and Antitrust Law hearing entitled, "Guilty until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point." As CFSA has previously stated in written testimony to the House Financial Services Committee both in April[2] and in July[3], we have grave concerns about Operation Choke Point trampling on the rights of legal and legitimate businesses in many different industries.

Operation Choke Point is a widespread federal program that has attacked countless businesses and industries, as well as the customers who rely on these lawful products. If Operation Choke Point is allowed to continue on its current path, the precedent that it is creating – that government regulators may secretly work to thwart lawful businesses and the customers they serve, without according them any due process rights – undermines the rule of law and is extremely concerning.

II. Operation Choke Point Effects on Consumers and Industry

While perhaps originally described as an attempt to prevent illegal bad actors from accessing the U.S. banking system, Operation Choke Point has gone well beyond attempting to keep fraud and criminal activity out of the

[1] CFSA was formed in 1999 to promote laws and regulations that protect consumers while preserving access to credit options and to support and encourage responsible practices within the payday loan industry. CFSA's member companies represent more than half of all traditional payday loan storefronts across the country, in more than 30 states. Our members provide payday loans to more than 19 million households, as well as a wide range of other financial products and services, including bill payment, check cashing, installment loans, prepaid debit cards, and tax preparation services. CFSA members' storefront locations put us in the heart of many financially underserved communities. CFSA members are heavily regulated at the federal level and in the individual states where they operate. Additionally, to serve our customers responsibly, CFSA has developed a set of 13 Best Practices that begin with compliance with all applicable state and federal laws. They cover everything from advertising to collection practices. Our members hold themselves to a higher standard, and we believe that these practices differentiate our members from other providers in the short-term credit industry.

[2] See CFSA statement to the House Financial Services Committee (April 8, 2014) available at http://gallery.mailchimp.com/24e3495ba13baf4c830a9e396/files/20140407_Written_Testimony_CFSA.pdf?utm_source=CFSA%3A+Membership+Updates&utm_campaign=8e5a140c0620140411_Membership_inReview4_11_2014&utm_medium=email&utm_term=0_cdf18bb939-8e5a140c06-215819909.

[3] See CFSA statement to the House Financial Services Committee (July 15, 2014) available at http://cfsaa.com/Portals/0/Testimony/20140714_Leg_House_Hearings_FS_WrittenStatement_CFSA_Final.pdf.

banking system. Rather, it appears to be an effort to prevent payday lenders and certain other legal but "disfavored" businesses from having banking relationships and automated clearing house ("ACH") business relationships, even though these businesses are operating legally as authorized by their state charters and licenses and in compliance with all applicable state and federal laws and regulations.

The Financial Fraud Enforcement Task Force (part of Department of Justice), the Federal Deposit Insurance Corporation ("FDIC"), the Office of the Comptroller of Currency ("OCC"), the Board of Governors of the Federal Reserve System ("The Board"), and potentially other regulators have been working together to pressure community banks and third party payment processors to reconsider use of ACH for online payday lenders. This unwarranted federal initiative does not distinguish between financial fraudsters and legitimate businesses that are operating legally. Rather, Operation Choke Point has extended its aim beyond bad actors and has taken aim at lawful products and services that regulators dislike or disfavor.

Operation Choke Point has expanded quickly with no apparent regard for the serious negative effects on consumers' access to responsible financial credit products. For the nearly 40 million underbanked consumers in our country, Operation Choke Point is limiting choices among responsible financial products, particularly for short-term, small-dollar credit. The breadth of Operation Choke Point extends throughout the nonbank financial services industry to numerous legitimate businesses that offer alternative consumer credit options, including payday loans, and has affected totally unrelated industries that regulators similarly dislike or disfavor.

III. Examples of Banking Terminations

There are numerous examples of banking institutions terminating their business relationships with dozens of payday lending clients, who are operating in full compliance with applicable law. Some of these banks specifically noted their concern that working with payday lenders was receiving heightened scrutiny from the prudential regulators. In other instances, the banks specifically cited "reputational risk" and "safety and soundness" as the bases for termination of business relationships with payday lenders. In most cases, however, these banks provided little to no detail or explanation regarding the reasons for the termination. Some banks merely stated that the decision had been made, citing no rationale for the decision or a vague reference to risk.

Below are several direct examples of CFSA member companies who have been negatively affected by Operation Choke Point. In all cases, the member has suffered financial burden by having to locate new banking institutions that provide the services it needs. In some cases, the members have not yet been able to replace these business relationships with banks. The following is just a sample of the statements and testimonials that CFSA has learned from its membership and others in the payday lending industry. Some of the examples do not identify the CFSA member by name out of respect for the company's understandable fear of additional adverse consequences.

Example 1 - Advance America

Year to date, Advance America has received terminations by nine different banks. Each bank independently informed the member that the service terminations were due to the result of pressure from its prudential regulator on the basis of reputational risk associated with the payday loan industry. The banks, Synovus Bank, Fifth Third Bank, Hancock Bank, Whitney Bank, Umpqua Bank, Capital One Bank, Cadence Bank, Citizens Bank, and RBS Citizens Bank had provided critical treasury management banking services to the member. Advance America had enjoyed good, long-standing business relationships with all of the banks. Three of the bank relationships had been in place for well over a decade.

Advance America's operations, performance and compliance programs had been more than satisfactory to these banks and the member had been in continuous communication with its banks about the reported heightened regulatory scrutiny of bank relationships with payday lenders. Advance America was surprised by the notices of termination since it had actually received assurances from two of the banks that, as one bank stated, "We were doing everything right."

Advance America depended on treasury management banks for access to payment, deposits, and ACH systems and networks, payroll processing, and other commercial treasury services. The terminations of these relationships disrupted the provision of credit and other services to consumers. Advance America believes it is clear that in accordance with Operation Choke Point, the prudential regulators are pressuring banks to terminate payday lenders' access to the banking system. Furthermore, it believes that regulators are not differentiating between those who operate in accordance with the law and those who do not.

Example 2 – Check Into Cash

Creditcorp (Check Into Cash) has had a longstanding relationship with a number of large national, regional and community banks. Until last year, the company maintained a syndicated credit facility comprised of approximately six banks. It also maintained depository services, bank branch services and other banking services with many hanks throughout the country.

Bank of America – Check Into Cash did business with Bank of America for 20 years and used over 250 of their bank branches. On March 19, 2013, Bank of America informed Check Into Cash it would not renew its loan credit commitment when Check Into Cash's bank credit facility expired in 2015. During the March 19 discussion, the Bank of America representative indicated that this was only a credit decision and it did not impact Check Into Cash's treasury relationship utilizing its bank branches and other services. Later in the year, however, Check Into Cash received a letter dated October 30, 2013 stating that Bank of America was terminating all banking services.

JP Morgan Chase & Co - On September 25, 2013, a representative contacted Check Into Cash stating that it too was terminating their banking relationship. The company received a letter dated November 12, 2013 confirming the bank's decision to close their accounts. The company had conducted business with JP Morgan Chase for 16 years.

Fifth Third Bank – Check Into Cash conducted business with Fifth Third for 19 years. The bank had been in Check Into Cash's bank credit facility. Check Into Cash banks with its branches and utilizes other banking services. Most recently, Fifth Third has been testing its safe recycler product in approximately 20 of the Check Into Cash locations, with plans to expand this to other centers. The bank also has been promoting the recycler program as treasury solution for Check Into Cash centers and a significant opportunity to expand the relationship with it. On March 5, 2014, Check Into Cash received a letter stating that Fifth Third Bank would be terminating the relationship.

All three of these banks indicated that the reason for closing the accounts was tied to payday lending. Since the company provides various other financial services such as short term installment loans, title loans, check cashing, etc., it asked if subsidiaries offering loans and services other than payday loans could continue to do business with the banks.

Example 3 – Cash Tyme

Cash Tyme operates in seven states, with approximately 50 storefront locations. The products it offers include payday advance loans and check cashing. Its banking relationships have been terminated by three different banking institutions in 2014 and has clearly suffered financial burden by trying to relocate to new banking institutions.

Capital One – Cash Tyme recently received a termination notice from Capital One Bank, in which the bank stated that it was terminating all deposit and treasury services with the company. The Capital One letter stated that the bank had "made the decision to exit the business of providing commercial banking services to check cashers and related businesses."

Fifth Third Bank – Cash Tyme had over a decade of business relationships which accounted for approximately $250,000 a year. It received a termination letter from Fifth Third earlier this year that stated that "services provided by clients in this industry are outside of our risk tolerance." This ter-

mination affected nearly 30 bank accounts. The member has not been provided additional information or a further rationale for the termination.

Wells Fargo- Cash Tyme had a long-time business relationship with Wells Fargo. It received termination letters from the bank earlier this year that terminated three different accounts, both deposit accounts and treasury management (ACH origination) services of those accounts. In a letter, the bank's explanation for termination was, "Wells Fargo performs ongoing reviews of its account relationships in connection with the Bank's responsibilities to oversee its banking operations. After careful review, a business decision has been made to close your account(s) referenced above and terminate all related Treasury Management services (e.g. ACH origination services) associated with the above accounts."

Example 4 – Speedy Cash, Inc. (Lending Bear)
Bank of America – Speedy Cash, Inc. was given verbal notification several months ago that Bank of America was "exiting the payday advance business," and would be closing its nine business checking accounts sometime in the next three to six months. Speedy Cash, Inc. finally received a written letter regarding the termination in late June, in which Bank of America stated it was closing all small business accounts with the company "based on the nature of your business and associated risks." The company has had difficulty finding another bank to take over these accounts.

Example 5 – Xpress Cash Management
Fifth Third Bank – Xpress Cash Management received a written termination notice from Fifth Third stating that the payday loan industry was "outside [its] risk tolerance."

Example 6 – CFSA Member Company A
The CFSA member company operates in 28 states, with over 1200 storefront locations. Among the products offered are payday advances, check cashing, installment loans, and title loans. The company had banking services terminated by four different banking institutions since December 2013 with very little reason provided.

BBVA Compass Bancshares – The bank terminated its relationship in December 2013. The company was told by the bank that they are no longer servicing the payday lending industry, providing no other specific reasons. This affected retail storefront accounts.

Bank of America- The bank terminated its relationship in December 2013. The company was told by the bank that it was ceasing to do business with the industry to avoid reputational risk and compliance issues, but it provided no more specific reasons. This affected retail storefront accounts.

JP Morgan Chase and Co – The bank terminated its relationship in February 2014. The CFSA member was told hy the bank that it was ceasing to do business with the industry to avoid reputational risk and compliance issues, but provided no more specific reasons. This affected retail storefront accounts.

Fifth Third Bank – The bank terminated its relationship in March 2014. The CFSA member was told by the bank that it was ceasing to do business with the industry to avoid reputational risk and compliance issues. The termination affected corporate accounts, retail storefront accounts, centralized returns, and the company's ACH processor.

Bank of California/ORCC – In September 2013, the company was informed by its card processing company that it could not continue to service payday lenders due to the unwillingness of its bank.

Example 7 – CFSA Member Company B
The CFSA member company is a lender for over 750 storefront locations. It has had two different banks terminate business relationships due to Operation Choke Point.

PNC Bank – The CFSA member has had 18 accounts terminated, with no specific reason provided for the termination. The bank just indicated that it was industry-related; no letter was provided.

Huntington Bank – The CFSA member has had 38 accounts terminated, with no specific reason provided for the termination. The bank just indicated that it was industry-related; no letter was provided. The company was only given 30 days' notice before the termination became effective.

Example 8 – CFSA Member Company C
Bank of America – The CFSA member lost its clearing and currency funding banking relationship with Bank of America. This covered 90 percent of its U.S. store network. The member's relationship with Bank of America originated with the founding of the company in the late 1990s. The member was given no advance notice, and the letter it received provided 90 days-notice.

Example 9 – CFSA Member Company D
Bank of America - In late November 2013, Bank of America notified this member that it would cease to conduct business with any payday lenders as of December 31, 2013. Since January, Bank of America has closed the company's accounts and they are currently operating without local banking because they have been refused service by several financial institutions

Example 10 – CFSA Member Company E
Bank of America – The CFSA Member had a long standing relationship with Bank of America, which was recently terminated. The member was told by Bank of America that it was no longer going to work with payday lenders because of compliance concerns. This member primarily offers installment loans and title loans, a fact that was shared with Bank of America. Bank of America still insisted on ending the banking relationship. Furthermore, it also closed an operating account with a management entity that does not, and never has, offered any loan products.

Example 11 – CFSA Member Company F
Huntington National Bank – The CFSA member company received a termination notice in May 2013. The member was told by the bank that they could not, "further discuss why Huntington has chosen to dissolve all banking relationships with payday lenders." However, the CFSA member believes it was related to Operation Choke Point.

IV. Conclusion

CFSA is extremely concerned about the adverse consumer and business impacts of Operation Choke Point. Our views are the same as many other organizations that serve the members of the industries that have been targeted: Operation Choke Point adversely affects the rights of legal and legitimate businesses through unwarranted and unjustified actions of federal agencies.

Operation Choke Point sets an extremely dangerous precedent if the federal government is permitted to be the moral arbiter of which industries deserve to be in business. It is imperative for the government to make every effort to differentiate fraudulent actors from legitimate, law-abiding businesses. Agencies of the federal government should not be permitted to take regulatory or supervisory action outside the letter and spirit of the laws passed by the Congress, and the banking system should not be used to deny lawful businesses due process and to favor certain industries, while punishing others.

We respectfully ask that Congress and this Committee take appropriate action to put an end to Operation Choke Point.

ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®

July 17, 2014

Operation Choke Point A Threat to Free Commerce and the Rule of Law

On behalf of the more than 6,500 community banks represented by the Independent Community Bankers of America, thank you for convening today's hearing on the Department of Justice's Operation Choke Point. We welcome this opportunity to submit ICBA's statement for the record.

Operation Choke Point is a DOJ initiative intended to address consumer fraud by "choking off" access to fraudsters' banking services. Community banks currently dedicate significant energy and resources to monitoring, detection and reporting of fraud and other financial crimes in compliance with the Bank Secrecy Act. Last year alone, depository institutions filed over 600,000 suspicious activity reports to assist federal and local law enforcement in the fight against financial crime. Community banks are eager to cooperate with law enforcement but cannot and should not act as police.

In the last two years, Choke Point has targeted more than 50 banks and payment processors with subpoenas issued under a very aggressive reading of its authority under the Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA). Reputation in their communities is the stock-in-trade of community banks. The mere prospect of enforcement action is daunting enough to lead risk adverse community banks to shut off access to their payment systems to all but the most established, low risk businesses.

All legal forms of business should be allowed to operate freely with access to essential banking services, subject to the discretion of banks, and without excessive pressure or intimidation from law enforcement. Law enforcement should focus on criminals directly, without forcing banks to act as police, and their efforts should be narrowly targeted. ICBA is encouraged that members of Congress on both sides of the aisle have been critical of the aggressive tactics and troubling impact of Operation Choke Point.

At the same time, bank regulators have begun applying unwarranted scrutiny to bank relationships with categories of businesses deemed "high risk" or that supposedly create "reputational risk." These businesses include internet-based businesses, short term lenders, telemarketers, debt collectors, and other lawful businesses. Regulators have questioned long-standing relationships with businesses that have been properly screened by the bank's own risk controls. It is beyond the scope of the supervisory process to assess a bank's reputational risk or to prohibit or discourage community banks from providing these services. Community banks are the best judge of their own reputation risk and have every incentive to safeguard their own reputations through proper screening of customers. They conduct due diligence to assess the

1615 L Street NW, Suite 900, Washington, DC 20036 ▪ 202-659-8111 ▪ Fax 202-659-9216 ▪ www.icba.org

level of risk of each customer relationship and ensure that controls are in place to identify and monitor these relationships on an ongoing basis.

The End Operation Choke Point Act of 2014 (H.R. 4986)

ICBA supports legislation that is currently pending in the Financial Services Committee that would preserve the ability of banks to serve legal and legitimate business customers without undue pressure from law enforcement or examiners.

The End Operation Choke Point Act of 2014 (H.R. 4986), introduced by Rep. Blaine Luetkemeyer (R-MO), would clarify responsibilities of cooperation between banks and law enforcement in cases of financial fraud. It would promote direct prosecution of fraudsters and preserve access to banking services for legal businesses. In addition, the bill would rein in DOJ's abusive use of subpoena authority and create a safe harbor for banks serving businesses that meet specific criteria.

Thank you again for the opportunity to provide this written statement for the record.

HEARING: GUILTY UNTIL PROVEN INNOCENT? A STUDY OF THE PROPRIETY & LEGAL AUTHORITY FOR THE JUSTICE DEPARTMENT'S OPERATION CHOKE POINT

U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON JUDICIARY SUBCOMITTEE ON REGULATORY REFORM, COMMERCIAL AND ANTITRUST LAW

July 17, 2014

Dear Chairman and Ranking Member:

My name is Marsha Jones, and I am the President of the Third Party Payment Processors Association (TPPPA). I am pleased to provide testimony on behalf of the organization and the industry.

Third-party payment processing is an integral part of the payments industry and the economy as a whole. Payment processors are the technology innovators that provide consumers faster and easier ways to make payments, and provide small and mid-sized businesses an opportunity to collect and make payments electronically. This enables them to compete more effectively in a global marketplace with their larger competitors. Third party payment processors also provide direct deposit of payroll, providing consumers with safe and immediate access to their paycheck.

A third party payment processor (TPPP) is a depository customer of a bank that processes payments on behalf of other companies (merchants) through the TPPP's banking relationship. The role of the TPPP is to provide merchants with access to the electronic payments system, so that the merchants' customers have the ability to make electronic payments to the merchant and the merchant can make electronic payments to employees (direct deposit of payroll) and their business partners (business-to-business payments.) Third party payment processors typically have hundreds of customers that they process for including, mom-and-pop grocery stores, day-care centers, homeowner associations and more. They also provide access to, and payment and technical support for tens of thousands of merchants for which payment processing directly through a bank would be cost prohibitive.

The most vulnerable of small businesses rely on third party payment processors to enable them to participate in electronic payments, as they may not meet the standards to set up direct payment processing services through a bank directly. For example, they may be too small to qualify to process payments through a bank, they are too new, or they are struggling to turn their company around and no longer meet the credit requirements of a bank to process payments. This category has grown significantly since the financial crisis. These are the primary business beneficiaries of third party payment processing.

Consumers rely upon third party payment processors for virtually all direct deposit of payroll, most innovative mobile payment solutions and many of the bills and online purchases that they make. Third party payment processors provide consumers with more electronic payment choices than credit cards. These expanded choices have become increasingly more important as consumers' access to credit has decreased, providing the opportunity for some vulnerable consumers, without access to credit cards, to continue to make electronic payments.

Like other financial institutions, third party payment processors seek a diverse portfolio of customers to help manage risk. If a payment processor elects to process for higher-risk merchants, the typical payment processor diversifies their payments portfolio with some higher risk and low risk transactions. This protects the processor and the bank from credit risk. However, the processor still has contractual and regulatory due diligence obligations that it has to meet with regards to these high risk merchants.

This third party role has become the subject of significant scrutiny by banking regulators and by the Justice Department, and appears to be the genesis of Operation Choke Point. Unfortunately, however, what appears to have started as a legitimate interest in targeting a few companies who may have facilitated fraudulent transactions has morphed into a significant attack on the whole industry. The impact of Operation Choke Point has been significant not only on the third party payment processors, and on the targeted, high-risk, and lawful industries that it seeks to disrupt, but also on the low-risk merchants that our members serve, as well as the consumers that benefit from the payment services.

Operation Choke Point is designed to sever the flow of funds to target merchants by separating either the processor or merchant from the banking system. However, when a processor is shut off from the banking system, ALL of their merchants are disrupted, including those for small businesses and direct deposit of payroll for consumers, resulting in harm to the economy and harm to consumers.

The strategy of Operation Choke Point causes severe collateral damage. Targeting a merchant by going after a payment processor that processes a wide variety of payments to businesses of all types as well as consumer payroll has far-reaching and devastating impact.

The Third Party Payment Processors Association is fully supportive of prosecuting merchants or processors who engage in or perpetuate fraud against consumers. However, we strongly believe Operation Choke Point has resulted in casting too wide a net and is an irresponsible and ineffective strategy.

The TPPPA recognizes that we have a responsibility to help our bank and processor members, and merchants they serve, to comply with the applicable laws and regulations. As such, we are voluntarily creating an industry best practices system as a means of self-regulating the third party payment processing industry. This Compliance Management System (CMS) will help enable banks and third party payment processors, as well as merchants to comply with the laws and regulation and ensure that proper due diligence is performed throughout the third payment processing system. We believe that this is the most responsible and effective way to impact change without disrupting innovation, hurting small businesses and robbing consumers of effective and innovative ways of making and receiving payments.

We thank the House Judiciary Committee for holding this important hearing and for the opportunity to present our written testimony.

"The hallmark of the TPPPA is promoting compliance as the road to achieve payments integrity and excellence." Marsha Jones, President, Third Party Payment Processors Association (TPPPA)

THIRD PARTY PAYMENT PROCESSOR ASSOCIATION (TPPPA)

The TPPPA is a national not-for-profit industry association representing and promoting the interests of payment and payroll processors, their financial institutions and their merchants. The TPPPA formed in the summer of 2013 to raise awareness of the unintended consequences of Operation Choke Point and to create industry best practices in compliance for third party payment processing.

The TPPPA was formed to address the unmet needs of payment processors and their financial institutions that primarily process Automated Clearing House (ACH) and remotely created checks (RCC) payments.

TPPPA Leadership

- President

Marsha Jones, AAP, NCP

- Board of Directors

Intercept (Fargo, ND)
Repay (Atlanta, GA)
ACHWorks (Gold River, CA)
EFT Network (Hawthorne, NY)
Secure Payments Systems (San Diego, CA)

President's Bio

- Accredited ACH Professional (AAP)
- National Check Professional (NCP)
- 6 years at Viewpointe Regional Payments Association (NACHA)

Member of NACHA's Risk Management & Advisory Group
Created and Facilitated Third-Party Sender Roundtable
Designed ACH Originator Compliance Self Assessment

- 7 years at Capitol Bancorp Ltd

Responsible for all payments processing for 50+ Community Banks

- 7 years at Wells Fargo Bank

Operations Manager Small Business Lending Renewal Team

Our Mission

In service of our members and the payments industry our mission is to provide:

- *Advocacy*
- *Leadership*
- *Support*

Advocacy

TPPPA advocates on behalf of its members as to the vital role processors play in our economy. Promoting and representing the interests of our members, and forging productive relationships with:

- Members of Congress
- Regulators
- Rule-Making Bodies (NACHA, ECCHO)
- Other trade associations, (ABA, ICBA, ETA, Regional Payment Associations)

Leadership

TPPPA provides leadership in the industry by working with stakeholders to explore opportunities and examine solutions to innovate in a compliant manner.

- Create industry best practices through our Compliance Management System.
- Engage members and industry stakeholders in the payments rulemaking.

Support

All TPPPA members receive exclusive and ongoing training, guidance and compliance support.

- Processor and Financial Institution members receive the Compliance Management System (CMS) as part of their membership at no additional cost.
- TPPPA supports other trade associations in their payments compliance efforts.

Code of Conduct

The Third Party Payment Processors Association is a not-for profit trade association responsible for providing advocacy, support and industry leadership to its members. The Association has adopted a Code of Conduct to ensure the activities that affect the payments industry and its members are conducted with the highest levels of integrity, professionalism and fairness. All active members of the Association will subscribe to the following Code of Conduct:

1. *Adhere to the spirit as well as the letter of all applicable regulations, rules and laws related to the payments it processes.*
2. *Avoid even the appearance of professional misconduct or criminal offense.*
3. *Conduct business in a manner that does not adversely impact the membership or the payments industry.*
4. *Conduct all activities in a professional and businesslike manner.*
5. *Remain current on financial obligations to Association.*
6. *Respect the privacy and confidentiality of the membership and member business.*

The Association reserves the right to disassociate itself from any organization that, in its opinion, fails to abide by our Code of Conduct.

Members Categories:

- Members (Voting and Non-Voting)
    - Payment Processors
    - Payroll Processors
    - Financial Institutions
- Affiliate Members (Non-Voting)
    - Merchants
    - Vendors
    - Other Associations
    - Other Industry Stakeholders

The TPPPA Compliance Management System

Policies that are tailored to the unique needs and responsibilities of TPPPA members:
Payment and Payroll Processors
Financial Institutions

Created to address the oversight of relevant regulatory agencies, including FDIC, OCC, FRB, CFPB and FinCEN

Processor Module
Written for payment and payroll processors policies incorporate guidance for:

Due diligence and enhanced due diligence
Ongoing monitoring, management and review
Detecting and reporting suspicious activity

Policies include:

BSA/AML/OFAC
Consumer Complaints
UDAAP
Information Security, Privacy, Red Flags
High Risk Verticals
Telemarketing, Debt Collections, Lending
And more

Financial Institution Module
Written for FIs with processors as customers. Helps incorporate existing policies of the financial institution into a cohesive program for third party payment processing.

Both Modules Address

Risk Assessment (Due Diligence and Underwriting)
Agreements
Merchant Training
Ongoing Monitoring
Periodic Review
Escalation and Reporting Suspicious Activity
Termination of Merchant Relationships

Regulator Interaction and Relationships

The TPPPA has conducted meetings with the following regulators to introduce them to the TPPPA and to socialize our Compliance Management System methodology:

Commission of State Bank Supervisors (CSBS)
Consumer Financial Protection Bureau (CFPB)
Federal Trade Commission (FTC)
Federal Depository Insurance Corporation (FDIC)
Office of the Comptroller of the Currency (OCC)
Federal Reserve Bank (FRB)

These meetings were productive and the following objectives were met:

- Introduced the association, our mission, purpose and immediate objectives
- Created an open dialog with regulatory agencies
- Created framework for sharing the TPPPA's CMS and receiving feedback

TPPPA's Commitment to the CMS

The TPPPA is committed to reviewing and updating the CMS on an ongoing basis to ensure alignment with changes to regulation, regulatory guidance and payment system rule changes. We are committed to continual improvement of the policy set and will add new policies as needed. For example, a policy for Remotely Created Checks and a policy for Managing Cross Channel is slated for the 2015 release. We are also committed to vetting the CMS with regulators and rule making bodies on an ongoing basis. The TPPPA will provide regulators with an initial copy of the CMS by August, 2104.

CMS Certification for Payment Processors

The TPPPA is in the process of developing control framework for a voluntary SSAE16 Certification Audit with an independent audit firm. Successful completion of a SOC1 audit in year one and SOC2 thereafter, will make processor eligible for certification by the association. The TPPPA CMS Certification Audit is estimated to be available in September 2014.

CMS Consulting and Training

The TPPPA provides consulting and training to assist members in integrating the CMS policies into their payments practices. We recognize policies alone do not make a difference unless they are used to align practices, processes and procedures with CMS policies, and have the policies drive the company culture and behavior. Ongoing training and support will be made available to the members to support the association's compliance objectives.

Contact Us:
Third Party Payments Processors Association (TPPPA)
20 F Street NW, 7th Floor
Washington, DC 20001
www.tpppa.org
Marsha Jones, AAP, NCP
President
(602) 402-0416 – Cell
mjones@tpppa.org

Questions for the Record from
Chairman Bachus
for the Oversight Hearing on
"Guilty Until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point"
July 17, 2014

Questions for the Honorable Stuart F. Delery

1. The Committee has received numerous reports of widespread client terminations within specific industries as a result of Operation Choke Point. Whether or not it was DOJ's intention, do you deny that it is happening?

2. ZestFinance is an online lending startup founded by a Princeton graduate who is the former Chief Information Officer at Google. It uses mathematical analysis of large consumer data sets to offer loans at a "far lower" cost than competing products. ZestFinance submitted a statement to the Committee that, as a result of Operation Choke Point, they have already had to lay off 45% of their workforce. Were you aware that this has been happening?

    a. If yes, how specifically has the Division responded? Has it met with company representatives or taken any corrective action, either in this case or more broadly?

    b. If not, are you worried about what similar cases you might be missing where Operation Choke Point is destroying innovation, killing jobs and harming the very people it is supposed to be helping?

    c. What specifically will the Division do to avoid further collateral damage of this kind?

3. The Comptroller of the Currency has lamented a trend toward "de-risking," the practice of "simply abandoning customers in higher risk categories because a lack of resources makes it difficult to manage the risk." Whether or not DOJ intended de-risking to occur as a result of Operation Choke Point, it seems clear that it is happening now. Accordingly, do you agree that DOJ can no longer claim this consequence is unintended if it allows Operation Choke Point to continue without changes? If so, what specific changes are you pursuing to avoid and reverse unnecessary de-risking?

4. In your testimony, you reference a 30% return rate as an indicator of fraud. At the hearing, a copy was produced of an Operation Choke Point subpoena demanding extensive records of processors & merchants with just a 3% return rate. DOJ has sent more than 50 subpoenas. What percentage of them demand information based on a 3% return rate or other rate lower than the 30% rate?

5. How precisely was that 3% benchmark developed? What was the financial expertise of those who developed it?

6. A memo to you about Operation Choke Point noted that DOJ may be "filing civil complaints or criminal cases against banks based on transactions with fraudulent merchants and/or

processors -- but not filing actions against the underlying fraudulent merchants or processors." How many lawsuits have you filed as a result of Operation Choke Point against the "underlying fraudulent merchants or processors"?

7. What alternatives to Operation Choke Point, better tailored to address fraud and avoid collateral damage, have you considered, or are you considering? For example, have you considered or are you considering establishing, safe harbors to facilitate cooperation with regulators, such as a safe harbor that would allow payments companies, which were not directly involved in the fraudulent activities of a merchant, to work with regulators without unnecessarily triggering an enforcement action.

8. At the hearing, we heard testimony that Operation Choke Point is merely enforcing long standing "know your customer" obligations under the Bank Secrecy Act. If so, why isn't the Financial Fraud Enforcement Task Force pursuing these cases under that statute and its implementing regulations instead of FIRREA?

9. Does federal law prohibit banks and other lenders from offering unsecured consumer loans with APRs that exceed 36% to consumers other than uniformed military personnel?

Questions from Subcommittee Ranking Member Henry C. "Hank" Johnson, Jr.

10. On June 26, 2014, Rep Luetkemeyer introduced H.R. 4986, the "End Operation Choke Point Act of 2014." How would this legislation affect the Civil Division's ability to investigate and prosecute unlawful activity and fraud on consumers?

Questions for the Record from
Chairman Bachus
for the Oversight Hearing on
"Guilty Until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point"
July 17, 2014

Questions for Adam Levitin

1. Your legal analysis of DOJ's FIRREA authority hinges on the involvement of the Automated Clearing House (ACH) system and its associated warranties and participation rules. Do you believe that the same analysis applies to the large number of non-ACH transactions also at issue in Operation Choke Point?

Questions from Subcommittee Ranking Member Henry C. "Hank" Johnson, Jr.

2. Under the Bush Administration, the Office of the Comptroller of the Currency, which plays an important role in the oversight and regulation of the financial system, issued guidance on several occasions noting the high-risk profile of third-party processors. Do you agree that this guidance issued under the Bush Administration demonstrates that the disparate treatment of lenders under state law and the opaque relationships of third-party processors continues to justify heightened monitoring and diligence requirements for banks transacting with high-risk merchants, such as lenders?

3. Do you believe that the guidance issued by financial regulators under the Bush Administration was a backdoor attempt to shut-down or "choke off" industries it did not agree approve of?

4. Has any guidance from financial regulators on high-risk merchants and payment processors departed substantially from the Bush-era guidance under the Obama Administration?

5. There is some concern that even if the Justice Department's investigations of unlawful activity is warranted, the mere act of sending administrative subpoenas to banks—or in the case of financial regulators, reminding banks of their anti-money laundering requirements—has caused unintended consequences resulting in banks no longer transacting with certain merchants in high-risk industries. Has this risk always existed in this industries, or has it risen substantially over the past several years as a part of the efforts of the Justice Department and financial regulators?

6. Jane Larimer, the general counsel of NACHA, has noted that allowing third parties to directly access the ACH Network exposes both financial institutions and the network "to a variety of risks, including frauds that arise out of shortcomings in the originators or third parties policies and procedures." As Larimer notes, when banks "abdicate all responsibility for risk management and they abdicate that due diligence responsibility, that definitely could add risk to the network." Was Four Oaks Bank one such example of a bank abdicating responsibility by allowing a processor to directly access the ACH Network on behalf of merchants despite overwhelming evidence of fraud and potentially unlawful actions?

Questions for the Record from
Ranking Member Henry C. "Hank: Johnson, Jr.
for the Oversight Hearing on
"Guilty Until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point"
July 17, 2014

Questions for Scott Talbott

1. Did the Justice Department provide an opportunity for the Electronic Transaction Association to meet with Assistant Attorney General Delery to express concerns associated with Operation Choke Point?

   ETA did meet with Assistant Attorney General Delery to discuss Operation Choke Point and its concerns about the adverse consequences it could have on payment processors, merchants and consumers. ETA also requested that the DOJ cooperate with payment processors to combat fraud, rather than adopt an adversarial approach through Operation Choke Point. ETA believes that a cooperative approach would be a more effective approach for preventing fraud while minimizing adverse consequences to law-abiding payment processors, merchants and consumers.

2. In your written testimony, you note the Electronic Transaction Association strongly supports keeping fraud off the ACH Network through existing laws and regulations. FIRREA is an existing law, correct?

   FIRREA is an existing law. ETA strongly supports using the proper authorities to combat fraud, but ETA is concerned about DOJ's use of FIRREA to pursue payment processors that were not committing fraud and holding them liable for fraud committed by third parties.

3. Courts have upheld the Justice Department's use of FIRREA to enforce existing laws and regulations to keep fraud off the ACH Network, correct?

   The case law on the applicability of FIRREA (12 U.S.C. § 1833a) with regards to payment processors is very limited. In particular, no appellate court has yet to rule on the scope of liability of payment processors under 12 U.S.C. § 1833a.

4. Are there high-risks associated with certain merchants and third-party processors?

   Some merchants may pose higher risks to consumers and the payment system based on the products they sell, their methods of sale, their location, and other risk factors. Nonetheless, these merchants may operate lawful businesses and engage in lawful sales practices. Payment processors already follow policies and procedures to evaluate and monitor these types of merchants to help mitigate risk and ensure that processors do not provide services to unlawful businesses. ETA has led efforts to further strengthen the

industry's due diligence and risk management practices through the development and promotion of its Guidelines on Merchant and ISO Underwriting and Risk Monitoring. (See answer to question 5 for more information on the ETA Guidelines). It is important to remember that ETA members bear the costs of fraudulent transactions and so have a strong incentive to keep fraudulent merchants off the payment system.

5. What are the Electronic Transaction Association *Guidelines*?

   The ETA Guidelines on Merchant and ISO Underwriting and Risk Monitoring provide tools and strategies to ETA members for the underwriting and risk management of merchants and the due diligence and oversight of independent sales organizations (ISOs) and other third parties. When used in conjunction with the rules set in place by existing payment networks, applicable laws and regulations, and the requirements of acquiring banks, the ETA Guidelines are intended to help prohibit unlawful merchants from entering into or remaining in the payment system.

6. On page 57, ETA's *Guidelines* discuss merchants requiring enhanced due diligence, including high-risk merchants. Which merchants are included in this category?

   The ETA Guidelines identify factors that payment processors can use to evaluate whether a merchant is likely to pose a higher risk of loss to the payment system or harm to consumers, including (among other things) processing performance of the merchant measured by sales volume, return transaction, and chargebacks; types of products sold; methods of sale; marketing tactics used by merchants; merchant locations; and newly identified fraud trends. The Guidelines pay special attention, for example, to e-commerce merchants, merchants that promote "free" and "free trial" offers, merchants engaged in membership clubs or continuity billing programs, telemarketing merchants, and merchants that use affiliate marketing. Section 3 of the ETA Guidelines (pages 19-29) provides a discussion of these merchants.

7. Do ETA's *Guidelines* also assume that there are high risks associated with certain merchants and third-party processors?

   The ETA Guidelines recognize that certain types of merchants may pose higher risk of loss to the payment system or harm to consumers. The ETA Guidelines focus on providing tools and strategies to evaluate these merchants and help the payment processor determine whether to provide services to these merchants. Section 6 of the ETA Guidelines also provide tools for ETA members that sponsor independent sales organizations (ISOs) and other third parties in reviewing and evaluating the practices of third party processors and their merchant portfolios. Consistent with recent guidance published by the Office of the Comptroller of the Currency, the Guidelines outline a number of risk considerations applicable to using third parties, including operational risk, compliance risk, credit risk, legal risk, strategic risk, reputation risk, and risks associated with the concentration of resources.

8. On page 58, ETA's *Guidelines* discuss reputation monitoring. What do ETA's *Guidelines* require of ETA's member organizations when "investigating merchants, particularly those representing potential higher risk due to marketing or sales methods, product type, or operational issues"?

   The introduction to the ETA Guidelines emphasizes that ETA members should use the Guidelines to prevent fraudulent merchants from entering into or remaining in the card acceptance ecosystem. With respect to merchant investigations, the ETA Guidelines advise ETA members to investigate fully, notate the merchant file completely, and take action concretely. The ETA member's action in response to an investigation will depend on the results of the investigation and may range from requiring the merchant to take corrective action within a specified time period to closing the merchant account. The ETA Guidelines clearly stress that increasing merchant reserves or charging higher fees to merchants should not be used as alternatives to requiring corrective action or closing accounts that pose unacceptable risk.

Questions for the Record from
Ranking Member Henry C. "Hank: Johnson, Jr.
for the Oversight Hearing on
"Guilty Until Proven Innocent? A Study of the Propriety & Legal Authority for the Justice Department's Operation Choke Point"
July 17, 2014

Questions for David Thompson

1. Setting aside any concerns that one might have with the usurious rates for borrowers of short-term loans, do you agree that unlawful lenders, or lenders operating in states without a license, are poor ambassadors of the short-term lending industry?

2. Do you agree that as unlawful activity, illegal lending in violation of state law should be investigated and prosecuted by state attorneys general, and where appropriate, the Justice Department?

3. Many of your members are engaged in services beyond payday lending, including money transmitting, correct?

4. Following revelations that terrorists utilized the U.S. financial system to launder money to finance the 9/11 attacks, the United States has worked to tighten controls over money laundering. Moreover, recent findings that banks like HSBC and BNP Paribas have been involved in unlawfully transmitting money to drug cartels, terrorists, and countries like Cuba and Iran in violation of U.S. sanctions, have heightened concerns about compliance with anti-money laundering rules. Do you think that it is inappropriate for a bank to avoid providing services to companies engaged in money transmitting if the bank either prefers to avoid that line of business or does not have confidence in the controls of a particular company?

5. In the only complaint filed by the Justice Department as a result of the Operation Choke Point investigations, did the Justice Department specifically target online lenders, or did the complaint more broadly apply to other unlawful activity, like Ponzi schemes and unlawful gambling?

6. In the Four Oaks Complaint, the Justice Department argued in paragraph 46, footnote five, that in addition to defrauding consumers, at least one of the online lenders that directly transacted with the ACH network through Four Oaks Bank was located in Georgia, a state where payday lending is strictly prohibited. Should this lender have been allowed to directly access the ACH Network through a bank in violation of Georgia's laws?

7. In its complaint against Four Oaks Bank, the Justice Department alleged that the bank provided payday lenders with direct access to consumers' bank accounts and the ACH Network. Upon further inquiry, Four Oaks Bank learned that Payday Lender 16 was owned by a resident of the United Kingdom. Four Oaks Bank also learned that Payday Lender 16 did not have a United States presence except for a mail-drop at a "virtual office" space. In April 2012, Four Oaks Bank concluded that Payday Lender 16 "appears to be a US company

in name only." Four Oaks Bank nevertheless provided Payday Lender 16 access to the ACH network, resulting later in 2012 in an astoundingly high return rate of 70.02 percent. Don't you agree that allowing merchants like Payday Lender 16 direct access to consumers' accounts is problematic, should be investigated, and prosecuted where unlawful activity is found?

8. Professor Levitin has argued that many of the harms complained of by high-risk merchants have occurred for more than a decade as a result of uniform treatment by financial regulators under both Republican and Democratic Administrations. How do you respond to this argument?

9. In your written testimony, you argue that financial regulation is arbitrary and capricious in violation of the Administrative Procedure Act. To which guidance are you specifically referring?

10. Under the Bush Administration, the Office of the Comptroller of the Currency, which plays an important role in the oversight and regulation of the financial system, issued guidance on several occasions noting the high-risk profile of third-party processors. For instance, in 2001, the OCC noted that banks need to understand the market and customer base of third-party processors whose "activities often involve significant reputation, strategic, transaction, and compliance risk to the bank." In 2001, the OCC also instructed national banks to be mindful of third parties seeking to avoid state laws that would otherwise apply to their activities lending laws, and to "take special care to avoid violating fair lending and consumer protection laws and regulations, particularly when the actual involvement of the bank and the third party may be invisible to the customer." How is this guidance any different than guidance by financial regulators under the Obama Administration?

11. Did the CFSA or other short-term lenders object to this guidance under the Bush Administration, or formally request a rulemaking under section 553 of the Administrative Procedure Act?

12. You also argue in your written testimony that short-term creditors are "an easy first target" for the DOJ's campaign against merchants disfavored by the current administration. Do you believe that the guidance issued by financial regulators under the Bush Administration was a backdoor attempt to shut-down or "choke off" industries it did not agree approve of?

13. Section 951 of Financial Institutions Reform, Recovery, and Enforcement Act, also known as FIRREA, authorizes the Attorney General to investigate and bring a civil action seeking civil penalties for substantive violations of, or conspiracies to violate, various criminal offenses, including wire fraud, that affects a federally insured financial institution. How does guidance by financial regulators have any relationship to the Justice Department's investigation of high-risk merchants under FIRREA?

14. Did the Justice Department use this or similar guidance from financial regulators as a legal basis for its complaint against Four Oaks Bank?

15. Did the Justice Department use this or similar guidance from financial regulators as a legal basis for subpoenas issued to banks under FIRREA through Operation Choke Point?

16. In the Supreme Court's recent case in *Michigan v. Bay Mills Indian Community*, the Court made clear that Native Americans "'going beyond reservation boundaries' are subject to any generally applicable state law"; that the state may "deny a license," and that if a tribe goes forward with unlicensed activities, the state has many powers "to shutter" illegal operations "quickly and permanently" illegal operation. The powers the Court cited include injunctions and criminal charges against individuals. In light of this ruling, do you think that it is inappropriate for a bank or processor that does not want to get caught in a dispute concerning tribal lending to avoid providing services to entities that rely on tribal authority to make loans to consumers off reservation without complying with state law?

17. Do you think it is inappropriate for a bank or payment processor to refuse to provide services to an entity that purports to be located in the Bahamas, Belize or another foreign country but provides services through the internet to consumers in the United State without complying with the state and federal laws that apply in those consumers' states?

○