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.

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).

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.

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]

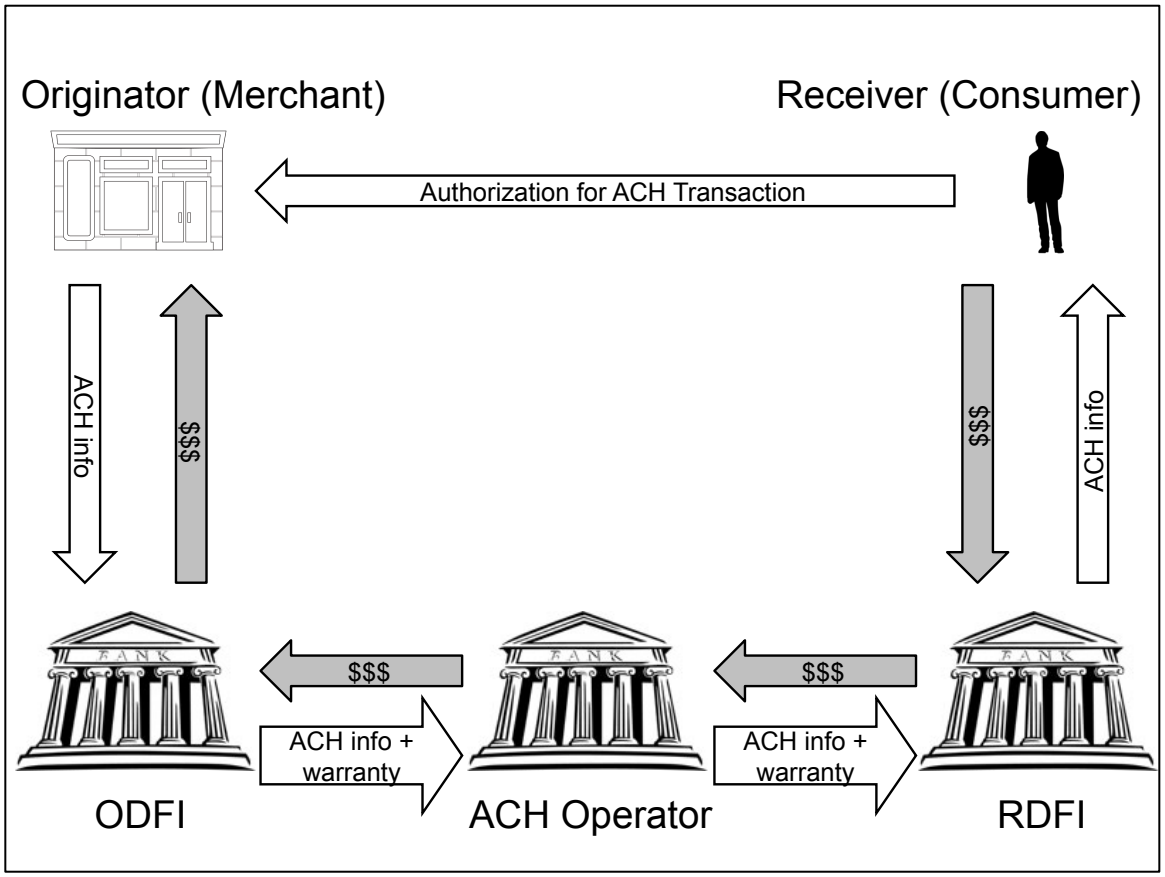
An ACH debit transaction involves an instruction to pull funds from a deposit account, whereas an ACH credit transaction involves an instruction to push funds from a deposit account. In an ACH debit transaction, the Originator (the payee) directs the ODFI to request that the RDFI transfer funds from 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.

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).

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

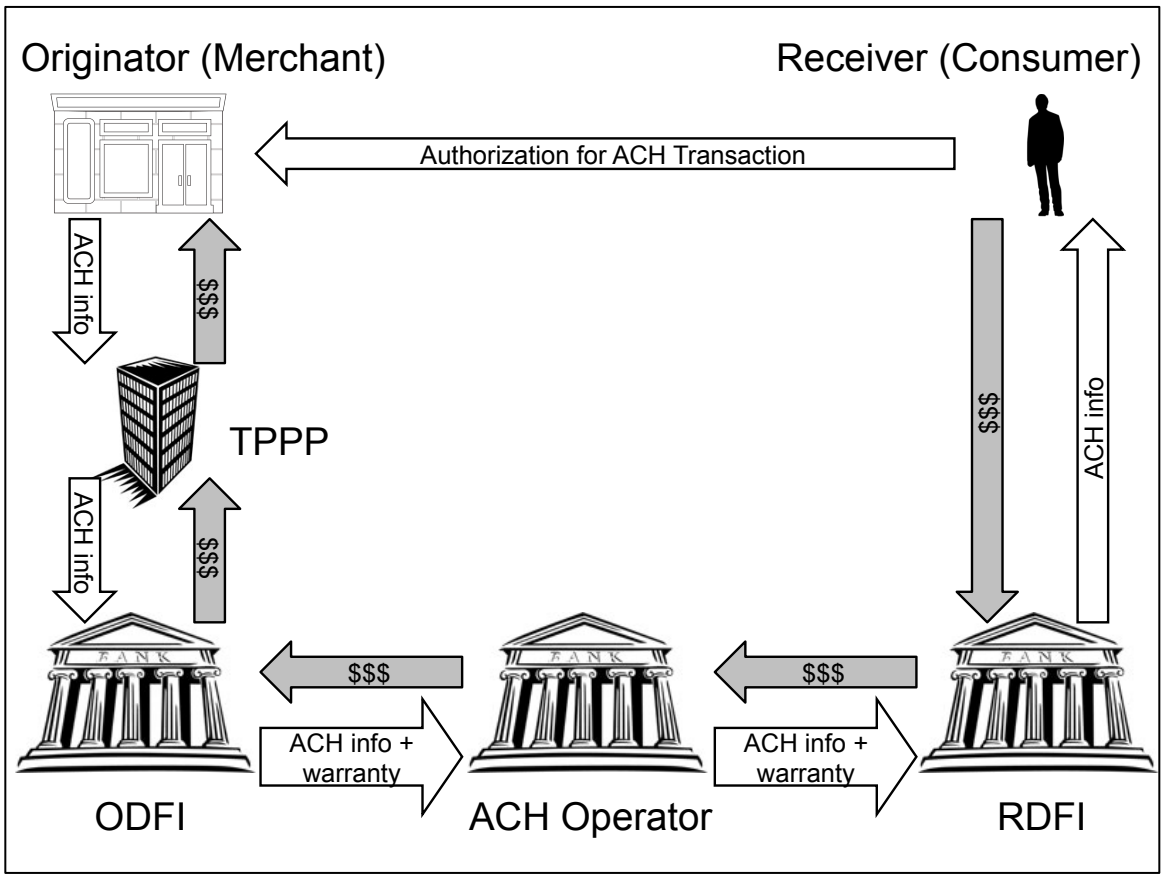
Some ACH transactions involve a Third-Party Payment Processor (TPPP). A TPPP serves as an agent for the Originator. The Originator will transmit the transaction information to the TPPP, which will in turn transmit the information to the ODFI. In some cases, TPPP are allowed to have direct access to the 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.

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.

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).

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.

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.

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.

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.