On
Supervision of Banks' Relationships with
Third Party Payment Processors
Before the
Subcommittee on Oversight and Investigations
Committee on Financial Services
U.S. House Of Representatives; U.S. House of Representatives;
2128 Statement of Federal Deposit Insurance Corporation
By
Richard J. Osterman, Jr.
Acting General Counsel Rayburn House Office Building
July 15, 2014

Chairman McHenry, Ranking Member Green and members of the Subcommittee, I appreciate the opportunity to testify on behalf of the Federal Deposit Insurance Corporation (FDIC) on the FDIC's supervisory approach regarding insured institutions establishing account relationships with third-party payment processors (TPPPs). I also will discuss the FDIC's interaction with the Department of Justice's consumer fraud initiative, Operation Choke Point.

As the primary federal regulator of state-chartered financial institutions that are not members of the Federal Reserve System, the FDIC is responsible for supervising these institutions for adherence with safety and soundness standards, information technology requirements, Bank Secrecy Act and other anti-money laundering laws and regulations, and consumer protection laws[1].

The USA PATRIOT Act, enacted in 2001, added new due diligence requirements for banks under the Bank Secrecy Act (BSA). Section 326 of the Act requires banks to establish and maintain a Customer Identification Program (CIP). At a minimum, financial institutions must implement reasonable procedures for: (1) verifying the identity of any person seeking to open an account, to the extent reasonable and practicable; (2) maintaining records of the information used to verify the person's identity, including name, address, and other identifying information; and (3) determining whether the person appears on any lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency. The purpose of the CIP is to enable banks to form a reasonable belief that they know the true identity of each customer. In its most basic form, knowing one's customer serves to protect banks from the potential liability and risk of providing financial services to an unscrupulous customer. In addition, but no less important, it provides another level of protection to the general public against illegal activity (including terrorist financing and money laundering) since banks are a common gateway to the financial system.

Certain kinds of businesses, transactions, or geographic locations may pose greater risk for suspicious or illegal activity. Higher-risk activities have been understood by industry[2] and the financial regulators as activities that may be subject to complex or varying legal and regulatory environments, such as activities that may: be legal only in certain states; be prohibited for certain consumers, such as minors; be subject to

varying state and federal licensing and reporting regimes; or tend to display a higher incidence of consumer complaints, returns, or chargebacks. Because these risks may be posed directly by a bank's customer, or indirectly through relationships established by bank customers with other parties (merchants, for example), banks have enhanced their customer due diligence policies and processes to better protect against harm. Harm to the bank can range from operating losses attributable to unanticipated consumer reimbursements that were not properly reserved for, to civil or criminal actions for facilitation of violations of law.

As challenging as it can be for financial institutions to understand the risks involved in the activities of a direct customer, the difficulty is magnified when the activities involve third parties. TPPPs may have relationships with hundreds or even thousands of merchant clients for which they initiate transactions. The vast majority of transactions passing through financial institutions and payment processors are legitimate transactions initiated by reputable merchants. These functions provide a valuable service to customers, both individual consumers and businesses, and are typically performed at a low cost. For example, banks often process customers' automated clearing house (ACH) transactions to credit or debit a bank account of another party as a service for their customers.

However, where transactions from the merchant client of a bank's TPPP customer are not legitimate, there is real risk for the bank because it can be held legally responsible for facilitating the activities and transactions of the TPPP. This is because in cases where the transaction was initiated by a third party, the bank still has a relationship, albeit indirect, with the TPPP's merchant clients, and thus would be exposed to the risks associated with their transactions. If the bank, through its customer relationship with the TPPP, is facilitating activity that is either impermissible in a state or being performed in a manner illegal under applicable state or federal law, the bank can be exposed to significant risks. As a financial regulator, the FDIC is responsible for ensuring that the financial institutions we supervise fully appreciate these risks, have policies and procedures in place to identify and monitor these risks, and take reasonable measures to manage and address these risks.

Supervisory Approach

Traditionally, TPPPs contracted primarily with U.S. retailers that had physical locations in the United States to help collect monies owed by customers on the retailers' transactions. These merchant transactions primarily included credit card payments, but also covered ACH and remotely created checks (RCCs). Guidance for FDIC-supervised institutions conducting business with TPPPs was contained within examination manuals and guidance related to credit card examinations, retail payment systems operations, and the Bank Secrecy Act.[3] However, as the financial services market has become more complex, the individual federal banking agencies, the Federal Financial Institution Examinations Council (FFIEC) and the Financial Crimes Enforcement Network (FinCEN) have issued additional guidance on several occasions warning financial institutions of emerging risks and suggesting mitigation techniques.

In December 2007, the Federal Trade Commission and seven state attorneys general initiated lawsuits against payment processors who processed more than $200 million in debits to consumers' bank accounts on behalf of fraudulent telemarketers and Internet-based merchants.[4] In April 2008, an insured financial institution that provided account relationships to payment processors whose merchant clients experienced high rates of return for unauthorized transactions or customer complaints of failure to receive adequate consideration in the transaction was fined a $10 million civil money penalty by its regulator. The penalty documents note that the institution failed to conduct suitable due diligence even though it had reason to know that the payment processors were customers that posed significant risk to the institution.[5] The Office of the Comptroller of the Currency and FDIC subsequently issued guidance that described the risks associated with TPPPs processing ACH and RCC for higher-risk merchants.[6] In 2010, the FFIEC updated the Retail Payment Systems Handbook to provide expanded guidance on merchant card processing and ACH and RCC transactions. The update provided a more in-depth discussion of the increased risks posed by these activities and some of the risk management tools that financial institutions can use to mitigate them.[7]

In late 2010 and through 2011, the FDIC observed TPPPs servicing disreputable merchants seeking to do business with small, troubled institutions.[8] This led the FDIC to issue expanded guidance in January 2012. In October 2012, FinCEN issued an Advisory noting that law enforcement had reported that recent increases in certain criminal activity had demonstrated that TPPPs presented a risk to the payment system by making it vulnerable to money laundering, identity theft, fraud schemes and illicit activity.[9]

A review of the relationships between banks and their customers or TPPPs is a regular component of the FDIC's examination process. Our supervisory approach focuses on assessing whether financial institutions are adequately overseeing activities and transactions they process and appropriately managing and mitigating related risks. Our supervisory efforts to communicate these risks to banks are intended to ensure that institutions perform the due diligence, underwriting and ongoing monitoring necessary to mitigate the risks to their institutions.

Where an institution is following the regulatory guidance and properly managing its account relationships with TPPPs, the institution has not been criticized. When we find that an institution is not properly managing its account relationships with TPPPs, the matter is discussed with bank management and noted in the institution's report of examination. If the deficiencies are not addressed, the bank may become the subject of an enforcement action to effect corrective action.

Most recently, in September of last year, the FDIC issued a Financial Institution Letter that clarifies and reminds financial institutions of the FDIC's policy and supervisory approach.[10] It states that financial institutions that properly manage relationships and effectively mitigate risks are neither prohibited nor discouraged from providing payment processing services to customers, regardless of the customers' business models, provided they are operating in compliance with applicable state and federal law. The FDIC re-emphasized this policy to address any confusion that may have existed about

our supervisory approach, and we have reiterated this policy to our bank supervision managers and examiners to ensure that examiners are following this policy.

In recent years, FDIC-supervised banks have heard from a number of state and federal agencies regarding the importance of ensuring that banks are properly managing their relationships with certain customers and third party payment processors. A number of states have expressed concerns about banks facilitating activities, especially online, that are illegal in their states. At the federal level, the Department of Justice (DOJ) also has actively contacted banks about similar issues. When the concerns and actions have involved FDIC-supervised institutions, the FDIC has cooperated with law enforcement and state regulators.

In early 2013, the FDIC became aware that DOJ was conducting an investigation into the use of banks and third party payment processors to facilitate illegal and fraudulent activities. From the FDIC's perspective, DOJ's efforts were aimed at addressing potential illegal activity being processed through banks. To the extent that the DOJ's actions were directed at potential illegal activity involving the banks that we supervise, the FDIC has a responsibility to consider the legality of certain actions involving our institutions as well as any potential risks such activities could pose for institutions we regulate.

The FDIC frequently coordinates with other agencies -- both federal and state -- in its supervision of our regulated institutions. Accordingly, FDIC staff communicated and cooperated with DOJ staff involved in Operation Choke Point based on an interest in DOJ's investigation into potential illegal activity that may involve FDIC-supervised institutions. FDIC attorneys' communication and cooperation with DOJ included requests for information about the investigation, discussions of legal theories and the application of banking laws, and the review of documents involving FDIC-supervised institutions obtained by DOJ in the course of its investigation. At all times, these attorneys worked for the FDIC and were performing their duties as lawyers for the FDIC in furtherance of the FDIC's mission.

In conclusion, the FDIC's supervisory approach focuses on assessing whether financial institutions are adequately overseeing activities and transactions they process and appropriately managing and mitigating related risks. Our supervisory efforts to communicate these risks to banks are intended to ensure institutions perform the due diligence, underwriting, and monitoring necessary to mitigate the risks to their institutions.

The FDIC does not and should not make business decisions for the banks that we supervise. Indeed, each bank must decide the persons and entities with which it wants to have a customer or business relationship. The FDIC has stated very clearly and publicly that financial institutions that properly manage customer relationships and effectively mitigate risks are neither prohibited nor discouraged from providing payment processing services to customers, regardless of the customers' business models, provided they are operating in compliance with applicable state and federal law.

Thank you and I am happy to take any questions.

---

[1]For state-chartered financial institutions that are not members of the Federal Reserve System with assets of more than $10 billion, the FDIC and the Consumer Financial Protection Bureau each have supervisory authority pursuant to certain consumer protection laws.

[2]https://www.paypal.com/us/webapps/mpp/ua/acceptableuse-full
https://payments.amazon.com/help/Amazon-Simple-Pay/User-Agreement-Policies/Acceptable-Use-Policy
https://support.google.com/wallet/business/answer/75724

[3]See FDIC Credit Card Activities Manual, http://www.fdic.gov/regulations/examinations/credit_card/index.html, June 12, 2007; FFIEC Retail Payment Systems Handbook, http://ithandbook.ffiec.gov/it-booklets/retail-payment-systems.aspx, February 25, 2010, (update to March, 2004 release); and, Federal Reserve, SR-93-64 (FIS), Interagency Advisory, Credit Card-Related Merchant Activities, http://www.federalreserve.gov/boarddocs/srletters/1993/SR9364.HTM, November 18, 1993; Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm, April 29, 2010 (most recent update to original June 30, 2005 release).

[4]See FTC Press Release, December 11, 2007, *FTC and Seven States Sue Payment Processor that Allegedly Took Millions form Consumers Bank Accounts on Behalf of Fraudulent Telemarketers and Internet-based Merchants.*

[5]See United States of America, Department of the Treasury, Comptroller of the Currency, AA-EC-08-13, In the Matter of: Wachovia Bank, National Association, Charlotte, North Carolina, Consent Order for a Civil Money Penalty.

[6]FDIC Financial Institution Letter, FIL-44-2008, *Guidance for Managing Third-Party Risk*, issued June 2008; and FDIC Financial Institution Letter, FIL-127-2008, *Guidance on Payment Processor Relationships*, issued November 2008.

[7]FFIEC, Retail Payment Systems Booklet, http://www.ffiec.gov/press/pr022510.htm

[8]See Consent Agreement between the FDIC and SunFirst Bank, St. George, Utah, dated November 9, 2010 (FDIC-I0-845b); Notice of Assessment issued by the FDIC in the matter of Fist Bank of Delaware, Wilmington, Delaware, dated November 16, 2012 (FDIC-12-306k); FTC Press Release, FTC Charges Massive Internet Enterprise with Scamming Consumers Out of Millions Billing Month-After-Month for Products and Services They Never Ordered, http://www.ftc.gov/news-events/press-releases/2010/12/ftc-charges-massive-internet-enterprise-scamming-consumers-out, December 22, 2010; FTC Press Release, FTC Action Bans Payment Processor from

Using a Novel Payment Method to Debit Accounts, http://www.ftc.gov/news-events/press-releases/2012/01/ftc-action-bans-payment-processor-using-novel-payment-method, January 5, 2012; FTC Press Release, Defendants Banned from Payment Processing, Will Pay $950,000 in FTC Settlement, http://www.ftc.gov/news-events/press-releases/2013/03/defendants-banned-payment-processing-will-pay-950000-ftc, March 13, 2013.

[9]FDIC Financial Institution Letter, FIL-3-2012, Payment *Processor Relationships, Revised Guidance*, issued January 2012; and Department of the Treasury FinCEN Advisory, FIN-2012-A010, *Risk Associated with Third-Party Payment Processors*, issued October 2012.

[10]Financial Institution Letter, FIL-43-2013, *FDIC Supervisory Approach to Payment Processing Relationships With Merchant Customers That Engage in Higher-Risk Activities*, issued September 2013.

Last Updated 7/15/2014