STATEMENT OF

MARTIN J. GRUENBERG
CHAIRMAN
FEDERAL DEPOSIT INSURANCE CORPORATION

before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
FINANCIAL SERVICES COMMITTEE
U.S. HOUSE OF REPRESENTATIVES

March 24, 2015

Chairman Duffy, 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 providing banking services to customers, including third-party payment processors (TPPPs). We are aware of concerns regarding the FDIC's efforts in this area and we welcome the opportunity today to clarify the FDIC's supervisory approach. I also will discuss the FDIC's interaction with the Department of Justice's (DOJ) Operation Choke Point.

As the primary federal regulator of state-chartered financial institutions that are not members of the Federal Reserve System, the FDIC supervises 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.

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 a customer engaged in fraudulent and unlawful activity. 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 gateway to the financial system.

Knowing your customer also involves ongoing monitoring of your customer base for signs of potential illegal activity, and when necessary, requires filing Suspicious Activity Reports (SAR) when banks believe a customer has engaged in a potential illegal activity. Regulatory guidance requires financial institutions to have a Customer Due Diligence (CDD) program that enables the institution to predict with relative certainty the types of transactions in which a customer is likely to engage. The CDD program assists the financial institution in determining when transactions are potentially suspicious, so that it can carry out suspicious activity reporting obligations. Banks, bank holding companies, and their subsidiaries are required by federal regulations, issued pursuant to the Annunzio-Wylie Money Laundering Suppression Act of 1992 to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:

- May involve potential money laundering or other illegal activity (e.g., terrorism financing).
- Is designed to evade the BSA or its implementing regulations.
- Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

TPPPs are bank customers that provide payment processing services to merchants and other business entities, and they often use their commercial bank accounts to conduct payment processing for their merchant clients. TPPPs are not subject to Bank Secrecy Act or anti-money laundering (BSA/AML) requirements, and therefore are not required to have customer identification programs, conduct customer due diligence, engage in suspicious activity monitoring, or report suspicious activity to federal authorities. As a result, some processors may be vulnerable to money laundering or other illegal transactions. It can be challenging for banks to monitor these accounts for suspicious activity, because TPPPs may have relationships with hundreds or even thousands of merchant clients for which they initiate transactions.

When a bank fails to identify and understand the nature and source of the transactions processed through an account, the risks to the bank and the likelihood of suspicious activity can increase. Accordingly, interagency regulatory guidance, which was first issued in 2005 and updated in 2010 and 2014, encourages banks offering account services to TPPPs to develop and

maintain adequate policies, procedures, and processes to address risks related to these relationships.[1]

If the bank, through its customer relationship with the TPPP, is facilitating activity that is performed in a manner illegal under applicable state or federal law, the bank can be held legally responsible. 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.

As a financial regulator, the FDIC is responsible for ensuring that the financial institutions we supervise fully understand these risks, have policies and procedures in place to identify and monitor these risks, and take reasonable measures to manage and address these risks. Accordingly, 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.

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

[1] See interagency guidance on examination procedures for Third Party Payment Processors, FFIEC BSA/AML Examination Manual, December 2, 2014. http://www.ffiec.gov/bsa_aml_infobase/pages_manual/olm_063.htm, originally issued June 30, 2005 and updated April 29, 2010.

automated clearing house (ACH) transactions and remotely created checks (RCCs). Guidance for FDIC-supervised institutions conducting business with TPPPs was issued as early as 1993 through interagency and FDIC examination manuals and guidance related to credit card examinations, retail payment systems operations, and the Bank Secrecy Act.[2] However, as the financial services market has become more complex and problems were identified, the individual federal banking agencies, the Federal Financial Institutions Examination Council (FFIEC) and the Financial Crimes Enforcement Network (FinCEN) have issued additional guidance on TPPPs on several occasions informing 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.[3] 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

[2] See 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; 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 Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm, December 2, 2014 (most recent update to original June 30, 2005 and updated April 29, 2010 releases).

[3] 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*.

processors were customers that posed significant risk to the institution.[4] The Office of the Comptroller of the Currency and the FDIC subsequently issued guidance that described the risks associated with TPPPs processing ACH and RCC for higher-risk merchants.[5] In 2010, the FFIEC updated the Retail Payment Systems Handbook to provide expanded guidance on merchant card processing, ACH and RCC transactions, and the Bank Secrecy Act/Anti-Money Laundering InfoBase to provide expanded guidance on banks' accounts with third party payment processors. The updates provided a more in-depth discussion of the management challenges posed by these activities and some of the risk management tools that financial institutions can use to mitigate them and continue to provide banking services.[6]

In late 2010 and through 2011, the FDIC observed instances of TPPPs targeting small, troubled banks to enter into business relationships in return for high fees. In certain cases where the banks lacked adequate controls to manage the relationship, banks were implicated in fraudulent activity.[7] This led the FDIC to issue an informational article to raise awareness of

[4] 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.

[5] FDIC Financial Institution Letter, FIL-44-2008, *Guidance for Managing Third-Party Risk*, issued June 2008; FDIC Financial Institution Letter, FIL-127-2008, *Guidance on Payment Processor Relationships*, issued November 2008; and OCC Bulletin 2008-12, *Payment Processors - Risk Management Guidance*, http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html, issued April 24, 2008.

[6] FFIEC, Retail Payment Systems Booklet, http://www.ffiec.gov/press/pr022510.htm; and Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm, December 2, 2014 (most recent update to original June 30, 2005 and updated April 29, 2010 releases).

[7] 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 First 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.

these risks in the Summer 2011 issue of the FDIC's *Supervisory Insights Journal*[8] and to issue expanded guidance on this topic in January 2012.[9] In late 2012, FinCEN issued an Advisory noting that "[l]aw enforcement has reported to FinCEN that recent increases in certain criminal activity had demonstrated that Payment Processors presented a risk to the payment system by making it vulnerable to money laundering, identity theft, fraud schemes and illicit transactions."[10]

The article and guidance were intended to describe the risks associated with financial institutions' relationships with TPPPs, and to provide guidance to insured institutions on appropriate risk management for relationships with TPPPs. Consistent with prior interagency and individual agency guidance first issued in 2005,[11] and in consideration of the rapid growth in ACH activity,[12] both documents contained examples of merchant categories that had been associated by the payments industry with higher-risk activity.[13] These examples were intended

---

[8] FDIC Supervisory Insights Journal, *Managing Risks in Third-Party Payment Processor Relationships*, Vol. 8, Issue 1. Summer 2011.

[9] FDIC Financial Institution Letter, FIL-3-2012, *Payment Processor Relationships, Revised Guidance*, issued January 2012

[10] Department of the Treasury FinCEN Advisory, FIN-2012-A010, *Risk Associated with Third-Party Payment Processors*, issued October 2012.

[11] See 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; OCC Bulletin 2006-39, *Automated Clearing House Activities - Risk Management Guidance*, http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html, issued September 1, 2006; Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering InfoBase, http://www.ffiec.gov/bsa_aml_infobase/pages_manual/manual_online.htm, December 2, 2014 (most recent update to original June 30, 2005 release); FDIC Credit Card Activities Manual, http://www.fdic.gov/regulations/examinations/credit_card/index.html, June 12, 2007; 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; OCC Bulletin 2008-12, *Payment Processors - Risk Management Guidance*, http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html, issued April 24, 2008.

[12] According to NACHA, https://www.nacha.org/ach-network/timeline, 7.53 billion ACH transactions were processed in 2003; 14.96 billion were processed in 2008 and 16.079 billion transactions were processed in 2011.

[13] 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

to illustrate trends identified by the payments industry and were not the primary purpose of the guidance, which was to describe the risks associated with financial institutions' relationships with TPPPs and how to manage that risk. Nonetheless, including these examples led to misunderstandings regarding the FDIC's supervisory approach to institutions' relationships with TPPPs, resulting in the misperception that some deposit accounts or banking relationships with specific categories of merchants were prohibited or discouraged.

Separately, in recent years, FDIC-insured 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.[14] At the federal level, 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 August 2013, I received a letter from Members of Congress expressing concerns that DOJ and the FDIC were pressuring banks and third party payment processors to terminate business relationships with lawful lenders. Upon inquiring, FDIC staff informed me that, in early 2013, staff at 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. As understood by the FDIC, DOJ's efforts, which DOJ referred to as Operation Choke Point, were aimed at addressing illegal activity being processed through banks. To the extent that the DOJ's

https://www.nacha.org/news/use-ach-network-illegal-internet-transactions
https://www.nacha.org/news/telephone-initiated-tel-entries

[14] For example, http://www.dfs.ny.gov/about/press2013/pr130806-link1.pdf.

actions were directed at illegal activity involving banks supervised by the FDIC, the FDIC has a responsibility to consider the legality of the activities as well as any potential risks such activities could pose for those institutions.

The FDIC frequently coordinates with other agencies -- both federal and state -- in its supervision of its regulated institutions. Staff informed me that FDIC attorneys communicated and cooperated with DOJ staff involved in these investigations based on an interest in any illegal activity that may involve FDIC-supervised institutions. As staff explained, FDIC attorneys' communication and cooperation with DOJ included responses to requests for information about the institutions under 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.

In order to address any concerns or confusion that existed about the FDIC's supervisory approach, we have undertaken a number of actions.

First, the agency issued a Financial Institution Letter in September of 2013 that clarified and reminded FDIC employees and financial institutions of the FDIC's policy and supervisory approach.[15] This guidance 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, provided the customers are operating in compliance with applicable state and federal law.

[15] 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.

Second, in July 2014, the FDIC took additional action to address continuing concerns about the inclusion in the article and guidance of examples of merchant categories that had been associated by the payments industry with higher-risk activity. As was discussed above, the examples of merchant categories in the FDIC's article and guidance were intended to be illustrative of trends identified by the payments industry at the time the guidance and article were released. However, the list of examples of merchant categories led to misunderstandings regarding the FDIC's supervisory approach to institutions' relationships with TPPPs, resulting in the misperception that the listed examples were prohibited or discouraged. To address these concerns, the FDIC issued a Financial Institution Letter restating its policy that insured institutions that properly manage customer relationships are neither prohibited nor discouraged from providing services to customers operating in compliance with applicable federal and state law. As part of clarifying the guidance, the FDIC removed the list of examples of merchant categories from outstanding guidance and the article.

In January 2015, the FDIC took additional actions to ensure that FDIC-supervised banks and bank supervision examiners and managers fully understand the FDIC's policies and expectations. We also established procedures to make certain that these policies and expectations are effectively implemented. These actions include the following:

- The FDIC issued a Memorandum to all supervision staff establishing new documentation and reporting procedures where the FDIC directs a financial institution to terminate deposit account relationships. The Memorandum makes explicit that the FDIC does not make business decisions, such as customer selection, for financial institutions and that insured depository institutions may provide financial services to any customer conducting business in a lawful manner. Institutions need only perform the due diligence,

underwriting and monitoring necessary to mitigate any risks that may be inherent in the relationship.

Under the new procedures, examiner recommendations for terminating deposit accounts can be made only in writing and must be approved in writing by the Regional Director before being provided to and discussed with an institution's management and board. Staff were directed that recommendations should not be made through informal suggestions. In addition, criticisms of an insured depository institution's management or mitigation of risk associated with deposit accounts that do not rise to the level of a recommendation or requirement for termination of accounts should also not be made through informal suggestions. The examiner recommendation must include the supervisory basis for why the termination is being recommended or required, including any specific laws or regulations the examiner believes is being violated. In addition, recommendations for terminating deposit account relationships cannot be based solely on reputational risk to the institution.

Regional Directors are required to provide quarterly reports to the FDIC Board of Directors and the Division Directors regarding requests or orders to terminate deposit accounts, along with the basis for such action.

- The Memorandum was communicated to all FDIC examination staff. I participated in a national call with all FDIC supervision staff where I described the new documentation and reporting requirements. In that call, I made clear the expectation of compliance with these requirements. I also met personally with the FDIC's six Regional Directors to emphasize the importance of following these procedures. In addition, the requirements will be emphasized at upcoming meetings and training sessions for FDIC supervisory staff.

  The FDIC established a new, dedicated toll-free number, 800-756-8854, and dedicated email box, bankingservicesOO@fdic.gov, for the Office of the Ombudsman for institutions concerned that FDIC personnel are not following FDIC policies on providing banking services. Communications with the ombudsman are confidential. Individuals or institutions also may contact the FDIC Office of Inspector General through its website at www.fdicoig.gov by using the "Hotline" button, by phone at 1-800-964-3342, or by email at ighotline@fdic.gov. The contact information for both the FDIC Ombudsman and the Inspector General were provided to all FDIC-supervised institutions in a Financial Institution letter.

- The FDIC issued a statement to all FDIC-supervised institutions on the practice of institutions indiscriminately terminating business relationships with certain categories of customers because of the perceived supervisory risk or heightened expense of maintaining the relationships, often known as "de-risking." This statement makes clear that the FDIC encourages institutions to take a risk-based approach in assessing individual customer relationships rather than declining to provide banking services to

entire categories of customers without regard to the risks presented by an individual customer or the financial institution's ability to manage the risk.[16]

- On December 17, 2014, I sent a letter to the FDIC's Inspector General (IG) requesting an examination of the allegations of misconduct by certain current and former FDIC employees (and any other individuals who might be identified by the IG) as part of the IG's ongoing investigation into activities surrounding Operation Choke Point that was requested previously by Members of Congress. I included a copy of the staff report of the House Committee on Oversight and Government Reform with the letter. Once the IG's factual findings are received, they will be reviewed to determine the appropriateness of any administrative action regarding the individuals still employed by the FDIC.

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. We have taken a number of significant steps to ensure that both our examination staff and our supervised banks understand that the FDIC will not criticize, discourage or prohibit banks that have appropriate controls in place from doing business with customers who are operating consistent with federal and state law. We also have established procedures to make certain that these policies and expectations are effectively implemented. We expect these efforts to be successful and are committed to addressing this issue.

[16] *Statement on Providing Banking Services*, https://www.fdic.gov/news/news/financial/2015/fil15005.pdf.