

For Release Upon Delivery  
10:00 a.m., July 15, 2014

TESTIMONY OF  
DANIEL P. STIPANO  
DEPUTY CHIEF COUNSEL

OFFICE OF THE COMPTROLLER OF THE CURRENCY

Before the

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS  
HOUSE COMMITTEE ON FINANCIAL SERVICES  
UNITED STATES HOUSE OF REPRESENTATIVES

July 15, 2014

Statement Required by 12 U.S.C. § 250:  
The views expressed herein are those of the Office of the Comptroller of the Currency  
and do not necessarily represent the views of the President.

## Introduction

Chairman McHenry, Ranking Member Green, and members of the Subcommittee, I have been invited to testify today as the Subcommittee reviews the Department of Justice's (DOJ's) Operation Choke Point investigation.

As the Deputy Chief Counsel for the Office of the Comptroller of the Currency, I have worked on Bank Secrecy Act and anti-money laundering issues for over 20 years. In my position, I represent the OCC on the Treasury Department's Bank Secrecy Act Advisory Group and the National Interagency Bank Fraud Working Group. Throughout my career, I have witnessed many cases where banks have been used, wittingly or unwittingly, as vehicles for fraud, terrorist financing, money laundering, and other illicit activities. Deterring such abuses is an important objective of our examination work and of the supervisory guidance we provide to bankers.

I appreciate having this opportunity to discuss how the OCC works to ensure that the institutions we supervise comply with federal laws and regulations, including the Bank Secrecy Act (BSA). However, the OCC is not part of Operation Choke Point and therefore my testimony will focus on the OCC's supervisory policies and actions.

It is OCC's policy to cooperate with law enforcement investigations and the OCC routinely receives and processes requests for information from law enforcement agencies. When not prohibited by law, the OCC provides other federal agencies, including the DOJ, with bank examination reports and other non-public OCC information when such information is requested by, and necessary for, those agencies to perform their official duties. Some of the official requests for examination reports and other non-public information the OCC received from DOJ during 2013 related to Operation Choke Point.

## OCC Supervision

The OCC's primary mission is to charter, regulate, and supervise national banks, federal savings associations, and the federal branches and agencies of foreign banks. In carrying out this mission, the OCC requires banks to soundly manage their risks, meet the needs of their communities, comply with laws and regulations, and provide fair access to financial services and fair treatment of their customers.

Banking institutions – large and small – play a crucial role in providing consumers and businesses across the nation with essential financial services and sources of credit that are critical to economic growth and job expansion. The safety and soundness of an institution can be threatened when a bank lacks appropriate risk management systems and controls for the products or activities it provides or the customers it serves. These controls are critical to ensure that our financial institutions are not used to perpetrate fraud, money laundering, terrorist financing, or other forms of illicit activity.

Currently there is great concern that banks are terminating the accounts of entire categories of customers, without regard to the bank's ability to manage the risks posed by those customers, and some have suggested that regulators are dictating those actions. As a general matter, the OCC does not recommend or encourage banks to engage in the wholesale termination of categories of customer accounts. Rather, we expect banks to assess the risks posed by individual customers on a case-by-case basis and to implement appropriate controls to manage each relationship. The Comptroller reiterated this message last March in a speech to the Association of Certified Anti-Money Laundering Specialists when he stated, "no matter what type of business you are dealing with, you

have to exercise some sound judgment, conduct your due diligence, and evaluate customers individually.”<sup>1</sup>

This is consistent with the approach the OCC takes in enforcing compliance with the BSA. The BSA and its implementing regulations require financial institutions to have systems and controls to appropriately monitor accounts for potential criminal violations and suspicious activity indicative of money laundering or terrorist financing. If we find significant weaknesses in a bank’s systems and controls, we will require the bank to take appropriate corrective action. In more serious cases, we will require corrections through an enforcement action. In rare cases where a customer has engaged in suspected criminal or other illegal activity, or the bank cannot properly manage the risk of an activity, we may order the bank through an enforcement action to terminate the customer’s account.

While we require banks to put appropriate controls in place to prudently manage their risks, outside of the enforcement context, the ultimate decision of whether to open, close, or maintain an account rests with the bank. In some cases, the bank may determine that it cannot effectively manage the risks on a cost-effective basis, and decide to close the account or exit a line of business. These are business decisions made by the bank itself and not dictated by the OCC. In fact, many banks have policies that call for them to close accounts based on certain criteria, such as after a certain number of Suspicious Activity Reports have been filed in connection with a customer, and we expect banks to comply with their own policies.

---

<sup>1</sup> Remarks by Comptroller Curry before the Association of Certified Anti-Money Laundering Specialists on March 17 available at <http://www.occ.gov/news-issuances/speeches/2014/pub-speech-2014-39.pdf>

### Payment Processors

The OCC recognizes the need for banks to provide services for a variety of customers, consistent with their business plans, and has issued bulletins on a wide range of topics to provide helpful guidance and best practices for banks to follow. For example, since the early 1990's the OCC has had in place principles for risk management for banks that maintain accounts for payment processors. These principles are embodied in guidance we issued in 2006,<sup>2</sup> which we subsequently updated in 2008<sup>3</sup> in connection with an OCC enforcement action against Wachovia Bank.<sup>4</sup> The OCC took this enforcement action in response to significant deficiencies in the bank's oversight of its business relationships with certain of its payment processor customers. Our 2008 updated guidance addressed the need for banks to have effective due diligence, underwriting, and monitoring systems in place for payment processors that are bank customers.

The Wachovia action is an example of the consequences a bank can face if it fails to implement proper controls to monitor and manage the risks posed by a customer's account. In this case, the OCC found that Wachovia failed to properly oversee the activity of third-party payment processor accounts despite significant red flags indicating consumers were being harmed by telemarketers that were the payment processors' customers. Many of the telemarketers deliberately targeted vulnerable populations, such as the elderly, using deceptive, high-pressure sales calls to convince these consumers to provide their personal checking account information to purchase products of dubious or

---

<sup>2</sup> OCC Bulletin 2006-39, "[Automated Clearing House Activities - Risk Management Guidance.](http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html)" <http://www.occ.gov/news-issuances/bulletins/2006/bulletin-2006-39.html>

<sup>3</sup> OCC Bulletin 2008-12, "[Payment Processors - Risk Management Guidance.](http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html)" <http://www.occ.gov/news-issuances/bulletins/2008/bulletin-2008-12.html>

<sup>4</sup> Formal Agreement, Wachovia Bank, N.A., Charlotte, North Carolina, and the Office of the Comptroller of the Currency, AA-EC-08-12 (April 24, 2008) and Consent Order for a Civil Money Penalty, Wachovia Bank, N.A., North Carolina, and the Office of the Comptroller of the Currency, AA-EC-08-13 (April 24, 2008).

no value. Payment processors used consumers' account information to create checks that were deposited into telemarketers' accounts at the bank. Because the consumers never received what the telemarketers promised, or funds were taken from their accounts without proper authorization, the bank received hundreds of complaints and hundreds of thousands of the checks created by the payment processors were returned to the bank.

Despite these significant red flags, and having clear knowledge that consumers were being harmed, the bank failed to properly address the situation. The OCC cited the bank for unsafe or unsound practices as well as unfair practices in violation of section 5 of the Federal Trade Commission Act, required it to pay approximately \$144 million in fines and restitution to consumers, and ordered other affirmative relief. The OCC did not require the bank to cease doing business with any third-party payment processors or telemarketers. Rather, the OCC's action was focused on requiring the bank to remediate specific consumer harm and establish enhanced risk management policies, procedures, systems, and controls to mitigate the risk of future harm to consumers.

#### *Money Services Businesses*

Press reports have indicated that banks have been terminating relationships with accounts of Money Services Businesses (MSBs). For banks that choose to open or maintain accounts for MSBs, the OCC has long taken the position that banks should apply the requirements of the BSA based on their assessment of risk, as they do for all customers, taking into account the products and services offered as well as any individual circumstances. Nine years ago, the Federal banking agencies and the Financial Crimes Enforcement Network (FinCEN) issued guidance clarifying our compliance expectations

for providing banking services to MSBs.<sup>5</sup> The guidance set forth our supervisory expectations for compliance with the requirements of the BSA and applicable state law.

Depending on its activities, an MSB can be considered a high-risk customer of a bank. The BSA requires financial institutions to conduct appropriate due diligence and review account documentation for all customers to determine whether the activity in these accounts is consistent with the customer's business or occupation and the stated purpose of the account. The purpose of these requirements is to ensure that the bank is not used to perpetrate money laundering, terrorist financing, or other illicit activity. Some financial institutions recently have elected not to offer accounts to high-risk MSB customers because of the costs associated with monitoring these accounts and ensuring compliance with the BSA. However, it is important to note that nothing in the BSA prohibits a financial institution from providing accounts to MSBs, even high-risk MSBs, as long as the institution's systems and controls are sufficient to effectively monitor the activity in these accounts.

### Conclusion

As a general matter, the OCC does not direct banks to open, close, or maintain accounts. Those are business decisions the bank must make for itself. But we require banks to put controls in place to manage the risks posed by their accounts. We recognize that banks need to make judgments about their risk tolerances and how they manage and control each customer relationship. Our reviews of a bank's controls are a matter of supervisory judgment. If the bar is set too high, it can cause a bank to terminate accounts of legitimate businesses. However, if the bar is set too low, the consequences can be dire,

---

<sup>5</sup> Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses operating in the United States, issued April 26, 2005; [http://www.fincen.gov/statutes\\_regs/guidance/html/guidance04262005.html](http://www.fincen.gov/statutes_regs/guidance/html/guidance04262005.html)

allowing the bank to be used as a vehicle to facilitate fraud, money laundering, terrorist financing, or other forms of illicit finance. Such activities can jeopardize the safety and soundness and even the viability of an institution. Consequently, we strive for a supervisory approach that is reasonable, balanced, and fair, and results in systems and controls that are effective in preventing and deterring the use of our nation's financial institutions for illicit purposes.