

Anti-Money Laundering Trends: Facts, Findings, and Lessons Learned

May 11, 2015



Increased anti-money laundering (AML) regulation enforcement by federal and state agencies in recent months should have financial institutions across the country reviewing and strengthening their in-house AML policies and procedures to prevent inadvertently entering law enforcement's crosshairs. Because filings by financial institutions required by the Bank Secrecy Act (BSA) play an important role in the federal government's efforts to detect and investigate money laundering and terrorist financing;^[1] failure by banks to make the appropriate filings or to monitor for activity that would trigger a filing under the BSA and implementing regulations will come under increased law enforcement scrutiny. Settlements in two recent actions brought by the Financial Crimes Enforcement Network (FinCEN), the Office of the Comptroller of the Currency (OCC) and the United States Department of Justice illustrate that financial institutions, both large and small, are subject to increased scrutiny from the agencies tasked with enforcing AML regulations. Below we examine settlements with Commerzbank AG and First National Community Bank Dunmore, Pennsylvania, which demonstrate the direction of emerging AML trends. **1. *Deferred Prosecution Agreement entered into by the Department of Justice (DOJ) and Commerzbank AG and Commerzbank AG New York (collectively, "Commerzbank")*** Facts On March 11, 2015, Commerzbank and the DOJ^[2] entered into a Deferred Prosecution Agreement (DPA) in settlement of Commerzbank's alleged violations of the International Emergency Economic Powers Act (IEEPA)^[3] and the BSA. For its violations of the BSA, specifically, its failure to (i) maintain an effective AML program, (ii) file suspicious activity reports, and

(iii) establish due diligence for foreign correspondent accounts; Commerzbank agreed to forfeit \$300 million in funds.[4] This was in addition to a \$79 million penalty and a \$263 million forfeiture for its IEEPA violations. *The DOJ's Findings* Commerzbank is a large international financial institution that conducts business in Europe, North America, and Asia; has 1,200 branches in Germany and 23 foreign branches, including one in New York. Commerzbank came under regulators' scrutiny when it was discovered that Olympus, a Japanese-based company, used Commerzbank as a conduit to perpetrate a massive accounting fraud that concealed from creditors and investors millions of dollars in losses. Commerzbank failed to file a suspicious activity report regarding Olympus, notwithstanding Commerzbank executives' stated suspicions regarding Olympus' dealings and massive transactions that caused the bank's AML monitoring software to issue alerts. The DPA provided that, although Commerzbank had an AML program in place, the program was riddled with inefficiencies, slow response times to AML system alerts, and poor communication among different branches' compliance officers. Compliance personnel at Commerzbank New York would routinely send, to other Commerzbank branches, requests for more information regarding automated AML-system alerts raised after the system detected a potentially suspicious transaction. These requests for information routinely went unanswered or inadequately answered by other branches, which, on certain occasions, resulted in Commerzbank New York simply closing the alert without requisite information or assurance that the transaction was not suspicious. These deficiencies made Commerzbank unable to ensure BSA compliance, or effectively prevent its branches from aiding in money laundering activities. Finally, the DOJ found that Commerzbank also failed to conduct basic due diligence of foreign correspondent banks and that transactions routed through these branches and affiliates could have aided in money laundering activity.

2. FinCEN's Assessment of Civil Money Penalty Against First National Community Bank Dunmore, Pennsylvania (FNCB) Facts On February 27, 2015, FNCB consented to the assessment of a civil penalty in the amount of \$1.5 million after FinCEN found that FNCB's conduct violated the BSA and its implementing regulations. *FinCEN's Findings* FNCB is a community bank in Pennsylvania with 19 branches and approximately \$1 billion in assets. FNCB failed to identify red flags and consequently timely report suspicious transactions. The red flags, which FinCEN alleges should have caused FCNB to conduct further review and analysis of related accounts—and ultimately file suspicious activity reports—include:

1. a law enforcement subpoena submitted in 2007 for information related to alleged criminal financial activity of an account holder who was also a FNCB board member and a former state court judge ("Conahan");
2. Conahan's purchase of a condominium through an entity, which was also an account holder at FNCB, where (i) in a short period of time, the value of the condominium was reported to have substantially and inexplicably increased and (ii) 12 weeks after its original purchase, Conahan personally refinanced the condominium, taking the entire payment in cash;
3. dramatic (quadrupled) increases in account holders' incomes where increased income was purportedly a result of rental income from a disproportionately high rental price for the property being rented;

4. the occurrence of large, round-dollar transactions among account holders at FNCB; and

5. the occurrence of large balance changes that occurred on a single day.

Many of the red flags identified by FinCEN arose before the criminal investigation of Conahan. However, once FNCB received the subpoena from law enforcement for information regarding Conahan, its awareness of his and his affiliates' accounts should have become more acute. Instead, FNCB failed to immediately analyze Conahan's transactions and report the suspicious activity. As a result, much of the funds derived from Conahan's criminal conduct were gone by the time authorities learned of the transactions. **Lessons Learned** As these settlements demonstrate, regulators are becoming increasingly aggressive in pursuing BSA violations. It is no longer the case that only financial institutions guilty of especially egregious behavior catch law enforcement's attention—institutions of all sizes are being scrutinized and must comply with each BSA requirement, or risk action by regulators. Given these developments, financial institutions should re-evaluate their AML policies and procedures to ensure they comply with the BSA and implementing regulations. Otherwise, they may face substantial penalties and forfeitures. Banks should review their AML compliance programs to make sure they are effective and vigorously applied in all circumstances. Additionally, financial institutions should conduct routine audits of AML compliance systems to ensure that they actually detect and alert bank employees to the existence of factors that would trigger the required filing of a suspicious activity report with FinCEN. As the Commerzbank and FNCB cases demonstrate, financial institutions—both large and small, domestic and international—must have vigorous and effective AML compliance policies, procedures, and practices in place to ensure BSA compliance. In addition, once a financial institution establishes an AML program, it must be vigilant in identifying, following up on, and reporting suspicious activity. Increasingly, as illustrated by these two recent settlements, financial institutions face significant and costly consequences for failing to take proactive AML steps. *Image source: Images Money (Flickr)*

[1] See *In the Matter of First National Community Bank Dunmore Pennsylvania*, Case No 2015-03, Assessment of Civil Money Penalty, 3 (U.S. Dept. of Treasury, Financial Crimes Enforcement Network February 27, 2015) (http://www.fincen.gov/news_room/ea/files/FNCB_Assessment.pdf).

[2] The parties to the deferred prosecution agreement are Commerzbank and the DOJ, Criminal Division, Asset Forfeiture and Money Laundering Section together with the U.S. Attorney's Office for the District of Columbia and the U.S. Attorney's Office for the Southern District of New York.

[3] Specifically, Commerzbank was found to have (i) systemically hidden its voluminous USD clearing business on behalf of Iranian banks—an activity prohibited by U.S. sanctions against Iran and (ii) processing significant amounts of USD transactions for Sudanese clients in violation of U.S. sanctions against Sudan. [4] *U.S. v. Commerzbank AG, et al.*, Deferred Prosecution Agreement (March 11, 2015) (link available at <http://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations-agrees-forfeit-563-million-and>).

Authored By



Adam P. Schwartz

Related Practices

[Securities Litigation and Enforcement](#)

[White Collar Crime & Government Investigations](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.