Fostering Financial Integrity -- The Role of Regulators, Industry, and Educators

Remarks by

Martin J. Gruenberg

Chairman

Federal Deposit Insurance Corporation

Case Western Reserve University School of Law

Financial Integrity Institute

New York, New York

March 23, 2017

Thank you, Professor Gordon and Deans Berg and Scharf, for inviting me to join you tonight. As an alumnus of the Case Western Reserve School of Law, I am honored to be here at the launch of the Financial Integrity Institute. I welcome the opportunity to discuss how the institute could help our nation's efforts to combat financial fraud, money laundering, and the financing of terrorism.

These crimes pose a critical challenge to the *integrity* of our financial system and the public's *confidence* in that system. They threaten the security of the system and, indeed, our *national security* more broadly. Identifying and reporting suspicious financial transactions, both here in the United States and abroad, are high priorities of financial regulators, law enforcement, and our national security agencies. They are essential to law enforcement's ability to fight drug trafficking, organized criminal activity, and, international terrorism.

While financial institutions ultimately are responsible for ensuring that their policies and activities are in keeping with applicable laws, regulatory agencies are charged with assessing compliance.

For both financial institutions and regulators, having people trained in these areas is critically important. The Financial Integrity Institute is offering a highly specialized degree that focuses on financial crime and is tailored for anti-money laundering (AML) professionals in both the private and public sectors. As far as I am aware, this is the first program of its kind. I commend the Law School for its initiative and leadership in this area and hope it serves as a model for the development of similar programs.

I would like to use my time this evening to talk about the issue of financial integrity from the perspective of a regulator. In particular, I will discuss the historical context for the laws

relating to money laundering and terrorist financing, the regulatory framework as it exists today, and key challenges that financial institutions face in carrying out their programs.

There is no question that efforts to combat financial crime are costly to undertake. Resources dedicated to financial integrity have grown over time as the scale and nature of the threat has increased and become more sophisticated. That is why regulators focus their efforts on the complexity and risk profile of institutions. It is also why a better understanding of how to combat financial crime is needed, and where the Financial Integrity Institute, in particular, has an important role to play.

The Evolution of the Problem and the Legislative Response

When Congress passed the Bank Secrecy Act, or BSA, in 1970, its original intent was to require banks to maintain certain records the government could use to support criminal and tax evasion investigations. Two problems were at hand: domestic financial institutions did not have the records or data needed by law enforcement, and citizens were using secret, foreign bank accounts for illegal purposes. Both problems boil down to a lack of data to prosecute crimes.

I would suggest that, over time, the problem has remained a lack of data, but the types of crimes being fought have grown in number, sophistication, and malicious intent. This has elicited legislative responses, bringing about the current BSA/AML framework. Let me take a moment to walk through the evolution.

After its initial enactment in 1970, the BSA was augmented 16 years later with the passage of the Money Laundering Control Act of 1986, which criminalized money laundering in the United States, prohibited the act of structuring transactions to evade reporting requirements, and required a review by regulators of BSA compliance for depository institutions during every

examination cycle. The act also authorized the federal banking agencies to issue regulations requiring BSA compliance programs, enforce certain standards in those programs, and take formal actions against institutions whose programs failed to meet the requirements of the BSA. Prior to this legislative change, the government could prosecute a financial institution for failing to file currency transaction reports for structured transactions, but was unable to prosecute the individual accused of the actual structuring. From my standpoint, the ability to prosecute the individual is critical to effective deterrence.

The BSA was augmented again a few years later following one of the earliest glaring examples of financial crime perpetrated by and through an international banking institution. The Bank of Credit and Commerce International (BCCI) was operating in 78 countries and held assets of more than $20 billion when regulatory and law enforcement authorities in a number of jurisdictions discovered that the bank was a massive conduit for money laundering and other financial crimes, and had illegally acquired a controlling interest in a U.S. bank.

The Senate Committee on Foreign Relations' 1992 BCCI Report noted the "extraordinary magnitude of international financial transactions," which at the time amounted to approximately $4 trillion per day that was moving through the New York clearance system alone.

An investigation of BCCI by the Foreign Relations' Subcommittee had begun in 1988, and investigators in the United States and the U.K. concluded that BCCI had been "set up deliberately to avoid centralized regulatory review, and operated extensively in bank secrecy jurisdictions." Before it was closed in 1991, BCCI had provided banking services to a number of senior foreign political figures, often referred to as "politically exposed persons," such as Saddam Hussein, Manuel Noriega, and Abu Nidal, as well as the Medellin Cartel.

The discovery of BCCI's criminal activity was a factor that prompted Congress to pass the Annunzio-Wylie Anti-Money Laundering Act in 1992. This law established recordkeeping requirements for certain funds transfers and added the suspicious activity reporting requirement. It also included a provision giving the federal banking agencies the authority to revoke banking charters and terminate deposit insurance for institutions convicted of a money laundering offense.

As the turn of the century approached, the Money Laundering and Financial Crimes Strategy Act of 1998 required the Treasury Department to develop and implement a national strategy to combat money laundering and related financial crimes and authorized the designation of high-risk money laundering and related financial crimes areas.

The attacks of September 11, 2001, underscored the relationship between financial crime and terrorist financing—terrorist groups use methods similar to those of criminal organizations to avoid transparency. It quickly became apparent that a key element in the fight against terrorism was identifying and reporting suspicious financial transactions that may be supporting international terrorism.

The 9/11 Commission Report found that the September 11th hijackers were able to finance their attack using bank accounts opened in their own names and with nothing more sophisticated than small wire transfers. Funds came from foreign countries, cash transactions were generally below reporting requirements, and at times debit cards were used by hijackers who did not hold the accounts.

Congress moved swiftly, and within a number of weeks passed the USA PATRIOT Act, formally known as the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act.

I think it is fair to say that the PATRIOT Act is the single most significant AML law that Congress has enacted since the Bank Secrecy Act itself. Among other things, the PATRIOT Act criminalized the financing of terrorism, authorized agencies to impose customer identification requirements on financial institutions, established information sharing regulations, and required enhanced due diligence by financial institutions for certain foreign correspondent and private banking accounts.

So what began as currency transaction reporting requirements to identify citizens evading tax payments has evolved into required BSA/AML compliance programs, suspicious activity monitoring, and new reporting requirements to identify money laundering and terrorist financing, among other financial crimes.

Anti-Money Laundering Framework

Provisions of the Bank Secrecy Act cover not only traditional depository institutions, such as banks, savings associations, and credit unions, but also non-bank financial institutions, like securities and commodities firms, loan or finance companies, money services businesses, insurance companies, operators of credit card systems, casinos, and dealers in precious metals, stones, and jewels. For this reason, a number of agencies supervise covered institutions and enforce the BSA.

Among these agencies is the Financial Crimes Enforcement Network, or FinCEN, which was established in 1990 to support law enforcement efforts and foster interagency and global cooperation against domestic and international financial crimes. The PATRIOT Act later re-established FinCEN as a bureau of the Treasury Department. FinCEN is now the designated

administrator of the Bank Secrecy Act and serves as the financial intelligence unit of the United States.

In its capacity as administrator, FinCEN issues regulations and interpretive guidance, provides outreach to regulated industries, supports the examination functions performed by federal and state agencies, and pursues civil enforcement actions when warranted. FinCEN's other significant responsibilities include collecting, analyzing, and disseminating information received from covered institutions, and identifying and communicating financial crime trends and patterns.

FinCEN has delegated much of its examination authority to regulatory agencies, including the FDIC and other federal banking agencies, the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC), and the Internal Revenue Service (IRS).

The federal banking agencies evaluate depository institutions for BSA compliance and are authorized to take a range of enforcement actions against depository institutions and individuals for compliance deficiencies. In addition, the FDIC has the authority to terminate deposit insurance for state-chartered banks—while the Office of the Comptroller of the Currency (OCC) has the authority to revoke national bank charters—for institutions that have been convicted of money laundering or terrorist financing. The FDIC has broad authority to terminate deposit insurance for any bank that engages in unsafe and unsound practices.

The SEC and the CFTC oversee participants in the securities and commodities markets, respectively, but their supervision and enforcement authorities differ. The SEC examines for BSA compliance and has both regulatory and enforcement authority under the federal securities

laws. Although the CFTC has authority to examine futures commission merchants and introducing brokers in commodities, it has only limited BSA enforcement authority.

Supervision of sectors that do not have a designated federal regulator, such as casinos and money transmitters, is delegated to the IRS, the National Indian Gaming Commission, and state-level regulators.

FinCEN, the federal banking agencies, and the SEC, may assess civil money penalties for BSA violations; however, the IRS Division of Criminal Investigations has authority regarding a wide variety of financial crimes, including money laundering, tax evasion, and the structuring of financial transactions in amounts to avoid reporting requirements,. This division works with the Department of Justice (DOJ), which has responsibility for civil and criminal enforcement authorities in this area.

All of these agencies seek to coordinate their efforts to ensure consistent approaches and treatment.

Regulatory and Supervisory Response

The FDIC's role in promoting and maintaining financial integrity has a number of dimensions, and largely involves on-site examinations and off-site monitoring of insured depository institutions in a range of safety and soundness areas. Because the nature of financial crime is always changing, the FDIC and other federal banking agencies also address emerging risks—like those presented by new products and services—through the supervisory process.

The FDIC's supervisory program includes a careful evaluation of an institution's compliance with the Bank Secrecy Act. We determine whether each depository institution has a board-approved BSA/AML compliance program that includes internal controls to ensure

ongoing compliance, independent testing, a designated BSA officer, and training, as well as a Customer Identification Program. History has shown that deficiencies in these areas can result in noncompliance with AML rules, failure to detect or address illicit financial transactions, and opportunities for insider abuse.

Our reviews also evaluate whether an institution has established a "culture of compliance." The BSA/AML compliance program failures we have seen often reflect a failure on the part of an institution's directors or senior management to establish a tone of compliance that permeates the institution. For this reason, we evaluate whether the directors demonstrate strong corporate governance, have a general understanding of the BSA/AML regulations and the risks posed to their institution, and that senior management and employees understand the importance of BSA/AML compliance.

The federal banking agencies are required by statute to use their cease-and-desist authority when an institution fails to establish or maintain a BSA compliance program or fails to correct any problem that was previously reported. The federal banking agencies also have the authority to assess civil money penalties when corrective action has not been achieved within a reasonable amount of time, or when serious violations or unsafe or unsound practices have been identified.

To highlight the relevance of BSA compliance and the impact on the U.S. financial system, I would like to provide a few examples of instances where the federal banking agency works in parallel with the DOJ to address unique cases. While the banking agency will assess an institution's control environment for preventing and detecting illicit financial transactions, including sanctions evasions, the DOJ will work with law enforcement to investigate possible criminal violations.

In the case of Riggs Bank, Washington, D.C., significant noncompliance with the Bank Secrecy Act ultimately led to its unplanned ending. The institution had multiple BSA/AML failures related to high-risk accounts, services, and customers, including foreign, private banking customers.

Riggs Bank facilitated transactions for Chilean dictator Augusto Pinochet and helped him hide millions of dollars in assets from international prosecutors. This activity was not reported to U.S. regulators or law enforcement authorities. Riggs Bank was assessed a civil money penalty of $25 million by federal regulators in May of 2004, pled guilty to one felony count for failing to file suspicious activity reports, and paid a criminal fine of $16 million in January 2005. This activity diminished public and regulatory confidence in the bank, forcing the sale of the institution in 2005.

In December 2012, HSBC Holdings Plc and HSBC Bank USA N.A. paid $665 million in civil penalties to federal banking regulators and entered into a deferred prosecution agreement with the DOJ. The agreement included the forfeiture of more than $1.2 billion, for its failure to maintain an effective BSA compliance program and to conduct appropriate due diligence on its foreign correspondent account holders. These failures enabled narcotics traffickers and others to launder hundreds of millions of dollars. HSBC Group also illegally facilitated hundreds of millions in transactions related to Cuba, Iran, Sudan, and Burma in violation of U.S. economic sanctions.

In May 2014, Credit Suisse paid nearly $2.6 billion to the DOJ, Treasury, and financial regulators for multiple BSA violations. Credit Suisse had helped clients use sham entities to hide undeclared accounts, structured transfers of funds to evade currency transaction reporting

requirements, destroyed account records sent to the United States for client review, and provided offshore credit and debit cards to repatriate funds in the undeclared accounts.

In June 2014, BNP Paribas S.A. was penalized close to $9 billion as part of a settlement agreement with federal and state government agencies for illegally processing financial transactions related to Sudan, Iran, and Cuba—all of which were subject to U.S. economic sanctions. BNP Paribas pled guilty to falsifying business records as well as conspiracy in connection to those falsifications.

Financial Institution Reporting

Fortunately, most institutions do not experience such BSA compliance programs failures. Their BSA/AML compliance programs are effective and allow for timely and comprehensive filings of currency transaction and suspicious activity reports.

FinCEN processes about 55,000 new filings daily from a wide range of filers—not just banks—and searches financial institution reporting for individuals, entities, and techniques used to launder money or finance terrorism. Information in the filings can be used to connect seemingly unrelated individuals and entities across the country and around the world. The financial intelligence derived from these searches is then disseminated to law enforcement and other relevant parties.

FinCEN has credited financial institution suspicious activity and currency transaction reporting in successful investigations of fraud schemes, drug trafficking, trade-based money laundering, foreign terrorist fighters, and the proliferation of weapons of mass destruction.

Still, the challenges faced by financial institutions in carrying out their critical role in this effort should not be taken lightly. Financial institutions bear a responsibility under the law to

monitor transactions and identify and report suspicious activity to law enforcement. We as regulators recognize that this responsibility is carried out at a cost. The evolving international and cyber dimensions of financial crimes further these challenges as money launderers, terrorist financiers, and other illicit actors use creative and increasingly sophisticated methods to adapt to changes in the financial, technological, and regulatory landscape. Going forward, lawmakers, regulators, and the financial industry will need to remain vigilant in our efforts to detect and prevent money laundering and other forms of financial crime, and balance the benefits of enforcement against the costs.

International Efforts to Combat Financial Crime

As the financial marketplace has become increasingly global, the volume and sophistication of financial transactions at the international level has risen, and new financial products and technologies have been introduced to facilitate these transactions.

The international dimensions of detecting and preventing financial crimes are not new. In 1989, the Financial Action Task Force on Money Laundering (FATF) was established by the G-7 Summit in response to growing concern about money laundering. This international group was charged with assessing money laundering methods and trends, establishing preventive measures, and developing standards to be used as guidance worldwide in governmental efforts to combat money laundering.

FATF issued its first set of Recommendations in 1990, less than a year after its creation, which was intended to provide a comprehensive and consistent framework to be used to fight money laundering. While FATF standards initially addressed money laundering, they were

expanded in 2001 to address terrorist financing, and were further revised in 2012 to address the financing of the proliferation of weapons of mass destruction.

One of FATF's primary tasks is to monitor the implementation of its Recommendations among FATF members. Member countries perform annual self-assessments and participate in a more detailed mutual evaluation process. During the mutual evaluation process, each member country is examined by a team of FATF assessors who determine the effectiveness of the country's system for monitoring compliance with AML and combatting the financing of terrorism (CFT) standards. The United States underwent such an assessment in 2016, and was found to have a "well-developed and robust anti-money laundering and counter-terrorist financing regime," according to the FATF report.

FATF also has a process for monitoring countries and jurisdictions that do not maintain adequate AML/CFT controls or do not cooperate in the global effort to prevent money laundering and terrorist financing. FATF's International Cooperation Review Group identifies and examines uncooperative jurisdictions and countries that have failed to implement effective AML/CFT systems, and it names those jurisdictions publicly.

In addition to FATF, the Egmont Group was formed in 1995, as an international body of financial intelligence units (FIUs). Membership is comprised of 152 FIUs, including FinCEN as the U.S. representative to the group. FIU members of the Egmont Group are uniquely positioned to cooperate and support international AML/CFT efforts through a platform for the secure exchange of expertise and financial intelligence.

As a counterpart to the international government groups, in 2000, a private organization known as the Wolfsberg Group organized to develop global AML/CFT guidelines for

international banks. To date, the Wolfsberg Group has issued 15 documents they call *The Wolfsberg Standards.*

New Technology, New Vulnerabilities

We all know that the continual adoption of new technologies, products, and services has long been a vital part of maintaining the competitiveness of financial institutions in a rapidly changing marketplace. But we also know that this evolution often brings with it new vulnerabilities. For example:

- A global financial system that facilitates cross-border transactions and international trade also provides an infrastructure that can further the reach of financial crime and effectively eliminates borders for bad actors.
- New payment technologies, like prepaid card programs, mobile banking, and digital currencies, connect populations without access to traditional banking services, but also can be used by criminals to instantaneously and anonymously move funds around the world.
- And the internet's prevalence allows for the swift transmittal of information, but expands the scope of identity theft schemes, which can be used by organized crime and terrorist groups to raise and launder funds.

While technological advancements may expose the industry to the risk of financial crime, they may also aid in better managing BSA/AML risks and monitoring for suspicious activities. For example, automated systems can flag unusual financial transactions and behaviors, manage

and reconcile customer due diligence data, complete identity verifications, manage data forensics, aggregate currency transactions, screen watch lists, and aid in developing institutional risk profiles. It is indeed a double-edged sword and illustrates the long-term nature of the challenges we face.

The Role of the Financial Integrity Institute

I would like to conclude my remarks this evening by underscoring the value of the Financial Integrity Institute.

I can speak from the experience of a financial regulator that one of our greatest human resource challenges is finding people with the requisite training, skills, and experience to carry out our critically important responsibilities to combat financial fraud, money laundering, and the financing of terrorism. These responsibilities require a high level of technical expertise, a broad strategic view, and frankly a sense of mission.

The institute, by offering a comprehensive curriculum dedicated to this field, is making an important contribution to safeguarding our financial system and our national security. I applaud the Law School for its leadership and look forward to watching your progress in the months and years ahead as you develop this program and hope it serves as a model for others.

Thank you very much.