

A nighttime photograph of a city skyline. A prominent skyscraper on the right side of the frame emits a powerful, vertical blue light beam that extends from the top of the image to the top of the building. The rest of the city is lit up with warm, yellow and white lights from windows and streetlights, creating a bokeh effect in the foreground. The sky is dark, making the light beam stand out.

Post-9/11 AML:
A Decade
of Rapid
Change

BY JOHN ATKINSON

IT'S BEEN 10 YEARS since the very tragic events of September 11, 2001, which have shaped our personal and professional lives in ways both large and small. For anti-money laundering (AML) compliance professionals, the past decade has been one of rapid change, and this 10-year anniversary of 9/11 is an appropriate time to look back upon the pivotal changes that have shaped the AML environment while also examining some of the emerging trends and issues that will influence our field in the coming years.

Compared to 10 years ago, more financial institutions—as that term is broadly defined under the Bank Secrecy Act (BSA)—are covered by more rules and requirements with greater regulatory scrutiny and higher penalties for noncompliance. New money laundering typologies and schemes have emerged, and technology applications allow deeper analysis of available data. As a consequence, financial institutions are devoting more time and resources to AML compliance than they were 10 years ago, though head counts have decreased overall in the past few years as part of the general belt tightening during the banking crisis. These long-term trends of “more and greater” seem likely to continue as criminals and terrorists respond to new detection and prevention techniques with creativity and persistence—an ongoing “cat and mouse” game.

So much has happened in the past decade that it is not possible to touch on every detail, but we will examine some of the major trends that have shaped where we are today.

Expansion of AML Regulatory Requirements

Shortly after 9/11, Congress passed the USA PATRIOT Act, Title III, which dramatically expanded the requirements of the BSA, the primary anti-money laundering law in the U.S. The USA PATRIOT Act contained many provisions to address the critical emerging issue of terrorist financing, which expanded the concept of money laundering to include ideological motives in addition to “for profit” criminal activity. At the same time, the act provided a platform for other AML-related rules and requirements to be implemented.

Although a regulatory proposal to put “know your customer” (KYC) requirements in place had been shelved only a few years before 2001 in response to overwhelming industry and public opposition, the USA PATRIOT Act enacted requirements that financial institutions develop a reasonable belief of the true identity of their customers. With additional guidance and best practice development from the Basel Committee on Bank Supervision and the Financial Action Task Force (FATF), as well as organizations such as the Wolfsberg Group, an organized and detailed approach to customer identification and acceptance has become standard operating procedure. This approach includes obtaining basic information to verify a customer’s identity, requesting additional information to understand and assess (usually by a structured rating system) the AML risk posed by a customer, developing an initial profile of expected activity, documenting greater amounts of information for those customers posing higher levels of risk, and keeping customer information up-to-date. Comprehensive customer due diligence (CDD) policies and procedures are considered the “cornerstone of a strong BSA/AML compliance program” by the regulators.¹

In addition to the expansion of the CDD/enhanced due diligence (EDD) requirements for customers generally, there has been recognition by regulators and the industry that certain customer types demand specific rules and attention. The role of foreign correspondent banks and bank-to-bank transactions in the money laundering and terrorist financing process has been recognized, and additional regulatory requirements for CDD and EDD on foreign correspondent banks have been implemented

SHUTTERSTOCK

to focus on shell banks, ownership structure, ownership commonality with other banks, supervisory oversight, and nature of customer base. Additionally, politically exposed persons (PEPs), while subject to scrutiny pre-9/11, have gathered more attention in the past 10 years as foreign corruption has become an increasingly important issue. The U.S. Senate Permanent Subcommittee on Investigations has been looking at this issue for many years, issuing detailed reports on Riggs Bank's involvement with Chilean dictator Augusto Pinochet and on the laundering of corruption proceeds in the U.S. by leaders of certain African countries. Recent political turmoil in the Middle East has brought foreign corruption to the forefront again with reports of the large offshore fortunes of ousted political leaders.

Other customer types that receive more due diligence in the post-9/11 era because of their potential money laundering or terrorist financing risk include charities, non-governmental organizations (NGOs), non-resident aliens (NRAs), foreign embassies and consulates, and nonbank financial institutions. A rigorous customer acceptance procedure that considers customer type and includes drilling through corporate structures, LLC ownership, and layers of private investment corporations (PICs) and international business corporations (IBCs) to find the true beneficial owner(s) is now standard practice.

The USA PATRIOT Act also expanded information sharing and reporting to the government and implemented voluntary information sharing among financial institutions. It further provided the Secretary of the Treasury authority to impose "special measures" on jurisdictions, institutions, or transactions that are of "primary money laundering concern," mandated quick access by law enforcement to bank records, and required AML programs to be considered in regulatory evaluation of applications for mergers and acquisitions, which elevated the strategic importance of maintaining a strong program. The USA PATRIOT Act Section 314(a) information request process has been very actively utilized, and as of July 2011 the Financial Crimes Enforcement Network (FinCEN) had processed 1,465 requests to financial information on subjects of interest. These requests yielded over 95,000 subject matches pertinent to 371 terrorist financing cases and 1,094 money laundering cases.

Expansion of Regulatory Coverage

While the requirements were expanding, the number and types of institutions having to implement AML programs (known as the "Four Pillars") or file suspicious activity reports (SARs) broadened considerably. The USA PATRIOT Act extended the AML program requirements to all financial institutions,² and implementing regulations have been written for most, though some, such as those for nonbank mortgage companies, are still pending. The following business entities have had SAR reporting requirements added since 2001:

- casinos (2002)
- broker/dealers (2002)
- currency dealers and exchangers (2003)
- futures commission merchants (2003)
- certain insurance companies (2005)
- mutual funds (2006)

Regulatory oversight for BSA/AML now involves a large number of governmental agencies at the federal and state levels, such as the Internal Revenue Service (IRS), the Securities and Exchange Commission (SEC), the Financial Industry Regulatory Authority (FINRA), federal and state banking regulators, and various state agencies regulating insurance, securities, and money services businesses.

Expanded Regulatory Guidance

While the new AML regulatory requirements imposed by the USA PATRIOT Act were being rolled out over several years, the banking regulators heard the cry for unified, written guidance to address industry concerns about conflicting recommendations and interpretations from field examiners. In 2005, the Federal Financial Institutions Examination Council (FFIEC) published the first edition of its *FFIEC BSA/AML Examination Manual*. This 200-plus-page manual was produced through extensive collaboration among the banking regulators, with significant input from FinCEN and the Office of Foreign Assets Control (OFAC), and it provided much needed and quite detailed guidance for bankers and examiners alike, especially regarding formal risk assessments, CDD/EDD, and suspicious activity reporting expectations.

Importantly, the manual included input from OFAC, which, as noted further on in this article, significantly stepped up its sanctions program updates and enforcement after the event of September 11, 2001. Similar to the AML guidance in the manual, the OFAC sections address assessing risks for OFAC transactions and designing a program to manage those risks. The *FFIEC BSA/AML Examination Manual* has been updated twice since its initial publication, and has become one of the most valuable tools available to AML compliance professionals.

Money Services Businesses (MSBs)³ have been hit from both sides in the past 10 years, both as sources of risk to other institutions as customers and as entities subject to AML program requirements and greater recordkeeping and reporting obligations in their own right under the BSA. To provide definitive AML program guidance to MSBs and their examiners, and to clarify expectations for financial institutions with MSBs as customers, FinCEN, the IRS, and other groups involved in MSB oversight issued in 2008 an examination manual specifically written for MSBs. Modeled after the FFIEC's manual, the *Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses* has also become an indispensable tool for AML professionals working for or with MSBs.

Expansion of Sanctions Requirements and Penalties

After 9/11, sanctions compliance became a more important part of AML programs at financial institutions. OFAC's sanctions programs addressing terrorism and weapons of mass destruction were amended and updated, and the lists of individuals and entities covered by these rules were significantly expanded and updates issued more frequently. Outside of the United States, the United Nations (UN) and European Union (EU) likewise expanded their sanctions programs. Because sanctions compliance is the responsibility of the AML officer in most financial institutions, it has become important for AML officers to stay abreast of changing programs and covered entities from mul-

multiple sanctions-issuing bodies. Additionally, the need for automated support for sanctions compliance has become absolutely critical because of the sheer volume of names on the many lists to be monitored, not to mention the volume and automated nature of many of the transactions (such as automated clearinghouse payments), which must be monitored for compliance with these programs.

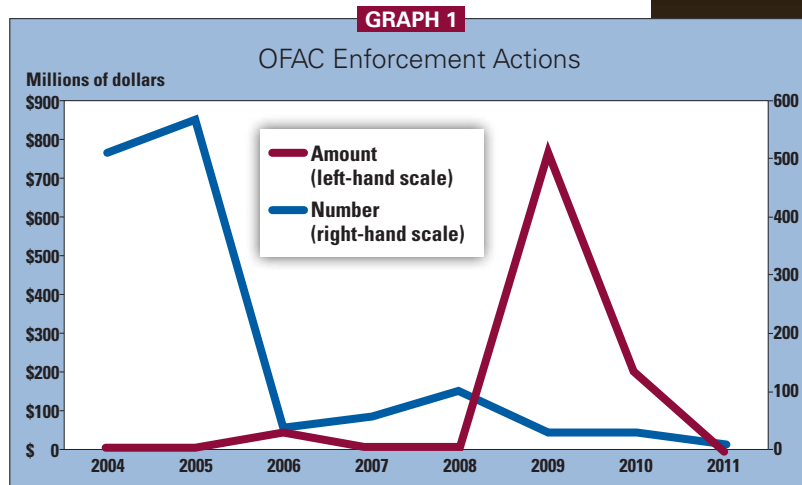
Over the past decade OFAC has both defined its enforcement program and stepped up penalties for noncompliance. In fact, some of the largest civil money penalties against financial institutions, including a few for hundreds of millions of dollars, derived from violations of sanctions laws. The largest penalties involved longer-term, large-scale issues of deliberate evasion of sanction program restrictions. Graph 1 shows the numbers and amounts of sanctions penalties from 2004 to 2011.

Expansion of AML Officer Duties

With all of these changes over the past decade, it is no surprise to those working in this field how the duties and expectations for AML compliance officers have expanded. In addition to keeping up with the new rules, regulations, and expectations for AML, it is common for AML compliance officers to have responsibility for sanctions compliance, Foreign Corrupt Practices Act (FCPA) compliance, fraud monitoring and reporting, communication with law enforcement, and compliance with the Unlawful Internet Gambling Enforcement Act (UIGEA). In smaller institutions, AML compliance officers often have broader consumer compliance responsibilities as well.

This breadth of duties now requires AML compliance officers to be knowledgeable of all business lines and operations within their institutions and how these areas and functions might be used to launder money, conceal illicit activities, disguise beneficial ownership, and transfer funds. Today's AML compliance officers are expected to have expertise in deposit products, loans, payments operations, trust and fiduciary products, securities operations, funds transmittals, insurance, trade finance, asset management, and more. In addition, they must develop an understanding of "normal" activity for the types of customers handled by their institutions to make decisions on whether transactions and activity are potentially suspicious and require filing a SAR. It is also necessary for AML compliance officers to stay abreast of international rules and issues, such as the U.K. Bribery Act and EU Directive on Money Laundering.

Because the scope of their responsibilities is so broad, AML compliance officers are now typically members of senior management, especially in larger institutions, and are expected to oversee an AML program covering all aspects of the entire organization, which can include multiple legal entities and business functions. This enterprisewide AML oversight should be a component of an overall enterprise risk management (ERM) program.



Greater Reliance on Technology

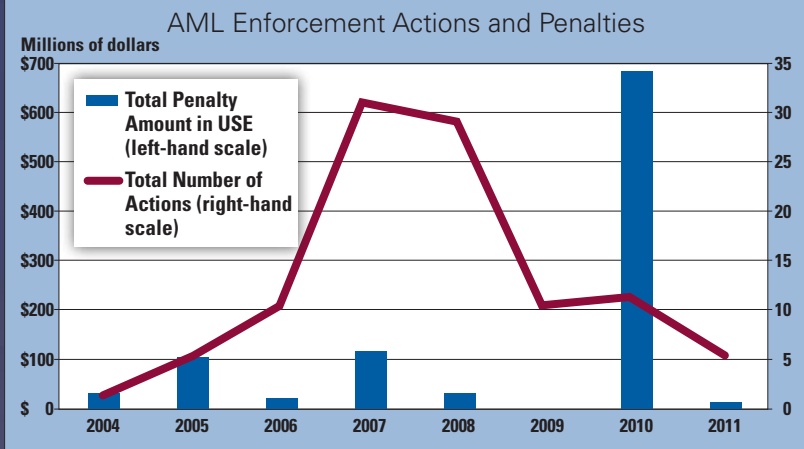
As regulatory requirements and expectations have grown, reliance on technology to support an effective AML program has grown as well. Except in the very smallest of institutions, automated systems are needed to analyze transactional data for patterns or indicators of suspicious activity, detect possible matches to names on sanctions lists, maintain CDD/EDD information for reference purposes, track investigations and cases, and maintain reporting data. Automated systems make it easier to aggregate activity across related accounts and to analyze data for money laundering typologies of current interest to the financial institution and law enforcement, such as mortgage fraud, Ponzi schemes, and human trafficking.

The benefits of technology do come with some costs and challenges. The need to install, maintain, upgrade, tune, and integrate AML systems now requires greater involvement from and collaboration with information technology (IT) professionals. Data quality is now a critical factor for program success, and the number of mergers and acquisitions among financial institutions in the past decade has placed a premium on being able to merge legacy systems in an efficient and effective manner. The regulators are focusing on system validation processes, data integrity, and automation needs planning.

Increased Risks for Noncompliance

Since 9/11, the regulatory agencies, in conjunction with FinCEN and law enforcement, have become more aggressive in issuing enforcement actions and assessing monetary penalties for AML programs that are deficient or allowed patterns of suspicious activity to go undetected. Graph 2 (next page) shows data from 2004 through 2010 on the number of formal enforcement actions and penalties assessed. These figures do not include the large volume of "informal" enforcement actions, such as memoranda of understanding,

GRAPH 2



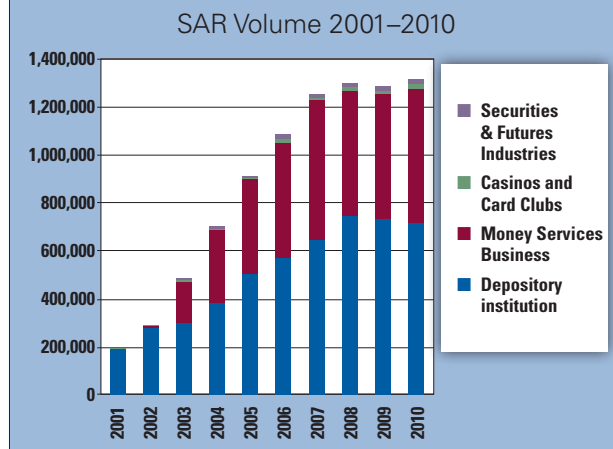
which compel corrective actions by a financial institution for AML issues. These data also do not show the additional, typically very large, expenditures by the affected financial institutions for legal counsel, outside consultants, additional in-house resources, and time devoted to compliance with the requirements of the enforcement actions and orders.

A review of enforcement actions over the past 10 years demonstrates that penalties have grown to dollar amounts routinely in the tens of millions. Institutions subject to enforcement actions have included banks both large and small, credit unions, money services businesses of all types, broker/dealers, and others. Penalties have even been extended to the individual level as officers and directors of banks have been personally fined for failure to correct deficiencies cited by their regulators. There is now more regulatory and law enforcement coordination on enforcement actions, with corrective actions and penalties determined by the collective actions of several regulatory/law enforcement entities.

One of the biggest changes in the enforcement action area since 9/11 has been the increased use of deferred prosecution agreements (DPA) by the Department of Justice. Under a DPA, criminal prosecution of a financial institution is set aside for some specified period, with the prospect of complete dismissal if the institution implements the corrective actions specified in the DPA. DPAs are used in conjunction with enforcement actions by other regulators, and the specified corrective actions are typically determined in a coordinated fashion. This prospect of criminal prosecution for money laundering violations is a very serious matter with consequences that could include the ultimate closure of the affected firm—a huge incentive to take corrective action in a forceful way.

Because of the importance of SAR data to law enforcement efforts, regulators started including “lookback” requirements in some enforcement actions to address situations where AML program deficiencies may have resulted in significant failures to detect suspicious activity. (See related lookbacks article on page 30). Institutions subject to lookback orders are required to review past transactions and customer activity to identify and report suspicious activity previously undetected because of AML program weaknesses. This is an expensive and resource-intensive endeavor,

GRAPH 3



and lookback orders, while still a common component of AML enforcement actions, have become more specific and targeted by the regulators to recognize this burden while still seeking productive results (and maintaining some measure of punitive value).

More Suspicious Activity Reports and Information for Law Enforcement

A fair question to ask at this point is whether all of these changes in the past 10 years have produced tangible benefits. Law enforcement certainly receives more data from 314(a) requests, SARs, currency transaction reports (CTRs), and other sources to use for investigations and prosecutions. Since 2001 SAR filings have increased by 674 percent, and exceeded 1.3 million in 2010 (see Graph 3). Feedback from law enforcement agencies through FinCEN’s *SAR Activity Review*, studies on typologies such as mortgage fraud, various agency presentations at industry conferences, and interactions with financial institution personnel demonstrate the value of SAR data in successfully initiating, investigating and prosecuting cases involving money laundering and its many predicate offenses.

What the Future Holds

As we look back over the past decade, there are very clear themes of more regulatory requirements, more entities subject to those requirements, higher regulatory expectations, better detection and more reporting of suspicious activity, greater consequences for risk management failures, and more demands on AML compliance officers. It’s dangerous to predict the future from the past, but there is little reason at this point not to expect these general trends to continue.

As far as particulars go, we see several areas that are likely to influence the AML environment over the next few years.

Technology. Financial institutions must manage enormous amounts data to run their businesses successfully, and speed and accuracy in execution will continue to provide a competitive edge. IT reliance will expand and improve, and over the next 10 years greater utilization of data, possibly from multiple institutions, will lead to more effective algorithms for specific typology

detection. Customer risk assessments will become increasingly accurate with more data and experience. Automated systems will have enhanced predictive capabilities to go along with stronger after-the-fact detection of suspicious activity. A reduction in “false-positive” alerts through enhanced technology would have very positive impacts on resource requirements and usage, and use of AML data and systems could enhance marketing strategies and improve profitability. Automation improvements will require AML compliance officers to be more technologically savvy and work even more closely with IT experts.

Payments Innovations. Innovations in payments and value transfer mechanisms have been rapid and creative, and will likely continue. Stored value cards, virtual currencies, and the use of mobile phones for direct transfers between consumers and/or businesses all present challenges for AML professionals to understand, monitor, and investigate, and challenges for governments to regulate on an effective and timely basis without stifling the marketplace. Many of these payments mechanisms require limited (or no) involvement by “traditional” financial institutions, such as banks, making these transactions less transparent to institutions with strong AML programs. Some of these new payments providers may find themselves coming under AML regulatory requirements, and more traditional institutions will need to adapt their AML programs to new and emerging payment methods.

Payments Monitoring. The UIGEA, though not a part of the BSA, is most often addressed by institutions’ AML programs to ensure proper monitoring and blocking of payments associated with unlawful Internet gambling. Congressional discussion in the past of similar payments monitoring and blocking requirements for other policy purposes (e.g., child pornography) leads to the belief that additional rules along these lines may be forthcoming. There are many challenges associated with identifying the purpose of individual transactions, and future payments changes will only compound these difficulties.

Know Your Customer’s Customer. While leading practice for AML risk management is to know your customer’s business strategy, types of customers, transaction expectations, and geographic territory, there has never been an explicit expectation that a financial institution should know the exact identity of its customer’s customers. The Comprehensive Iranian Sanctions, Accountability and Divestment Act of 2010 (CISADA) makes clear that there are circumstances that will require a financial institution to know (or at least make a good faith effort to inquire about) the exact and true identity of its correspondent bank’s customers, both at the account and payment transaction level. The value to law enforcement and government agencies of being able to look through a “window” at one institution at the customers of another institution may prove valuable enough to expand the notion and application of KYCC.

Interagency Cooperation/International Cooperation. The benefits of cooperation on AML matters have become very apparent to the many regulatory and law enforcement agencies that oversee

financial institution compliance or use the records and reports produced. Although this cooperation is not always perfect, we will likely see continued cooperation and coordination in the future on rulemaking, information sharing, and punishment for transgressions. On the international front, we can expect continued cooperation through groups such as FATE, Basel Committee for Bank Supervision, and others to promote consistency in AML risk management on a global basis. It is also likely that the trend of information sharing among governments for criminal investigations will continue, with expansion of information sharing related to tax issues, especially when government finances are under pressure.

Global Events. We live in a world where money flows easily around the globe, and events in other countries can influence local businesses and consumers. Global events will play an important role in AML risk management in the future as businesses leverage international connections to take advantage of new opportunities and as consumers move funds to locations offering greater safety, higher returns, or more confidentiality. These events, as in the past, may include political upheaval or changes, tax law modifications, exchange controls, nationalization of industries, or even amendments to money laundering laws.

Summary

While the details of the future are virtually impossible to predict, professionals working in the AML field fully recognize that new challenges will continue to arise and that meeting these challenges will require flexibility, adept use of technology, and cooperation with peers, regulators, and law enforcement. Without a doubt, there will be headaches and hardships caused by resource constraints, enforcement actions, new requirements, and money laundering innovations. However, the recognition that a greater good is produced by our collective efforts to detect and prevent money laundering, terrorist financing, and all of the associated criminal activity keeps us all motivated and energized. ■

ABOUT THE AUTHOR

JOHN H. ATKINSON, CAMS, is a Director in Protiviti’s Regulatory Risk Consulting Practice. Protiviti provides internal audit and risk & business consulting services to companies worldwide. Prior to joining Protiviti three years ago, Atkinson had a long career in bank supervision at the Federal Reserve Bank of Atlanta. The author acknowledges the contributions of his Protiviti colleagues Carol Beaumier and Mike Brauneis. John can be reached at john.atkinson@protiviti.com or (404) 926-4347.

Endnotes

¹FFIEC BSA/AML Examination Manual, p. 63.

²USA PATRIOT Act, Section 352.

³MSBs include check cashers; currency dealers or exchangers; issuers, sellers, or redeemers of traveler’s checks, money orders, or stored value cards; and money transmitters. See 31 CFR 103.11(uu) for complete definition.

Without a doubt, there will be headaches and hardships caused by resource constraints, enforcement actions, new requirements, and money laundering innovations.