Financial Crime: How Financial Institutions Can Mitigate Risk and Improve Compliance

Banks face dramatically higher operating costs and business complexity, with the increased scope of financial crimes and growing regulatory liabilities, highlighting the need for a more integrated and unified approach to risk mitigation and compliance.
Executive Summary

Top financial industry executives are increasingly concerned about the rising sophistication of financial crimes, including money laundering, terrorism financing, cybercrime, fraud, tax evasion, bribery and internal threats from employees. At the same time, the number of banks being penalized for regulatory and sanctions violations in the U.S., the UK, the European Union and elsewhere has spiked in recent years, demanding greater transparency, responsibility and compliance. Furthermore, the increase in extra-territorial enforcement of U.S. laws and reciprocation from other countries has amplified compliance challenges, vastly increasing the cost and complexity of doing business.

Banks have made huge investments in risk and compliance management, but their fragmented approach to financial crime has had limited success in staving off threats and meeting regulatory requirements. This has resulted in increased violations and money spent on regulatory compliance.

Clearly, banks need to refresh their approach to handling financial crime and regulatory compliance. We recommend six key steps to help banks adapt to the ever-changing criminal and regulatory landscape.

- **Conduct a risk assessment** based on the bank’s products, services, geographies and clients to better understand the threat environment.

- **Integrate the efforts of various disciplines involved in financial crime prevention** across the organization to identify synergies and overlaps in people, processes and technologies; this will help reduce redundancies and streamline processes.

- **Improve the availability and quality of data** to support real-time transaction monitoring and advanced analytics.

- **Apply advanced analytics** to gain a holistic view of threats and the entities that cause them; this will help uncover complex and subtle threats, as well as emerging ones, early and effectively.

- **Nurture a culture of high ethics and integrity** by setting accountability standards, establishing controls and policies, working closely with regulators and increasing employee awareness.

- **Actively participate in the industry-wide initiatives** undertaken to mitigate risk and improve compliance.

The Growing Burden of Financial Crime and Regulatory Compliance

Criminals are more sophisticated than ever when it comes to financial and cybercrime, and banks are struggling to catch up. Meanwhile, increased regulatory demands for transparency and compliance, as well as hefty penalties for non-compliance, have put enormous pressure on banks, both financially and operationally.

Rising Threats

A number of drivers — including globalization, the proliferation of banking channels, rising transaction volumes and accelerated technology advancements (i.e., new digital tools and intelligent automation) — have introduced new

---

**Single Biggest Barrier to Fighting Financial Crime Effectively for UK Banks**

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evolving criminal methodologies</td>
<td>42%</td>
</tr>
<tr>
<td>Cost of AML compliance</td>
<td>15%</td>
</tr>
<tr>
<td>Lack of personnel in risk function</td>
<td>15%</td>
</tr>
<tr>
<td>Civil prosecution/class actions</td>
<td>11%</td>
</tr>
<tr>
<td>Geo-political events</td>
<td>10%</td>
</tr>
<tr>
<td>Sectoral sanctions</td>
<td>10%</td>
</tr>
</tbody>
</table>

*Base: 198 senior-level financial crime and AML compliance professionals
Source: The British Bankers’ Association and LexisNexis, November 2015
Figure 1*
opportunities for financial malfeasance. Criminals continuously probe banking organizations’ defenses through innovative algorithms and complex schemes across channels and vectors; banks must also guard against internal employee threats (see Figure 1, previous page).

Big banks are not the only targets; small banks are easy prey for criminals, as many lack robust systems to fend off threats.

**Heightened Regulatory Scrutiny and Surging Compliance Costs**

Regulators across the globe have intensified their scrutiny and are assessing heavy fines to banks that fail to adopt adequate defenses or that violate the Banking Secrecy Act/Anti-Money Laundering (BSA/AML) program. Between 2007 and 2014, banks paid about $21 billion in cumulative anti-money laundering (AML) fines alone in the U.S.!

Banks are continuously challenged by emerging AML compliance requirements (see Figure 2). This includes the long-awaited beneficial ownership rule from the Financial Crimes Enforcement Network (FinCEN), expected to be finalized this year, which will require banks to verify and identify the true owner of companies behind financial transactions. Banks will also need to understand the implications of the ongoing assessment of the U.S. Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) framework developed by the Financial Action Task Force (FAFT).

In response to the 2001 terrorist attacks, the U.S. significantly expanded the scope of laws governing money laundering, bribery and fraud and applied them extra-territorially; the European Union and the UK followed suit. The EU’s Anti-Money Laundering Directive (AMLD 4) – which will be implemented by member states starting June 26, 2017 – requires financial institutions to continuously identify, evaluate and document risks related to money laundering and terrorist financing; report suspicious transactions made by their clients; and maintain records of payments.

Sanctions compliance is another major challenge for global banks as they strive to keep pace with a dynamic sanctions list comprising individuals, countries and institutions, separately maintained by the EU, the U.S. and organizations such as the United Nations. Banks must also keep up with lists for AML, tax evasion and other forms of crime. The growing list of individuals and entities to be screened has put pressure on banks’ transaction screening systems, increasing the number of false positives generated. U.S. authorities have clamped down on foreign banks for lax controls over financial crime and sanctions; European banks are most affected by this crackdown (see Figure 3, next page).

In the UK, the Financial Conduct Authority (FCA) has increased its scrutiny and updated its guidance on financial crime prevention. The move was based on a 2014 review of 21 small banks, which found significant weaknesses in the AML systems and controls in high-risk situations at most banks;
additionally, staff at one-third of the banks lacked awareness of AML and sanctions risks.²

Further, regulators want banks to take greater responsibility for preventing financial crime and reporting suspicious activities. In response, banks have made efforts to enhance their transaction monitoring systems, acquire greater knowledge about customers and their transactions, and recruit people with expertise in risk investigation and compliance.

The shortage of trained compliance specialists and the increasing responsibilities of compliance professionals – who assimilate an average of 167 regulatory alerts per day, a sharp increase from 68 a few years ago – are forcing banks to offer higher salaries to find and retain the best talent. This has vastly increased costs, with the largest global banks spending about $4 billion a year on compliance.³ Amid demands from customers and investors to lower costs, global banks have terminated certain products, services and customer relationships in high-risk segments and geographies.

For resource-constrained small- and medium-size banks, regulatory compliance has become a particular concern, with costs at many banks spiraling out of control. Many of these institutions have not updated their compliance programs, especially for BSA/AML, although they are held to the same expectations as their larger counterparts.

Challenges of Fighting Financial Crime
Keeping up with accelerating regulatory change is proving difficult for banks, but non-compliance can be even more costly. Costs include monetary fines, remediation, termination of business lines and temporary or permanent restrictions on selling certain products, not to mention the unquantifiable impact of investor dissatisfaction and reputational damage to the brand.

Banks have invested heavily in strengthening security and meeting compliance demands, but such efforts are undermined by their piecemeal approach to dealing with financial crime. Risks such as money laundering, cybercrime and fraud are traditionally handled independently by various organizational functions. Each has its own tools, systems, processes and compliance mechanisms, with minimal communication among them.

This fragmented approach has resulted in duplication of data, technology and efforts, resulting in rising costs. The largest global banks spend an estimated $1 billion to $1.5 billion annually on financial crime compliance.⁴ Without consolidated data from

<table>
<thead>
<tr>
<th>Bank</th>
<th>Year</th>
<th>Fine (in $ million)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BNP Paribas (France)</td>
<td>2014</td>
<td>8900</td>
</tr>
<tr>
<td>Standard Chartered (UK)</td>
<td>2013</td>
<td>667</td>
</tr>
<tr>
<td>ING (The Netherlands)</td>
<td>2012</td>
<td>619</td>
</tr>
<tr>
<td>Credit Suisse (Switzerland)</td>
<td>2009</td>
<td>536</td>
</tr>
<tr>
<td>ABN Amro (The Netherlands/UK)</td>
<td>2010</td>
<td>500</td>
</tr>
<tr>
<td>HSBC (UK)</td>
<td>2012</td>
<td>375</td>
</tr>
<tr>
<td>Lloyd's (UK)</td>
<td>2009</td>
<td>350</td>
</tr>
<tr>
<td>Commerzbank (Germany)</td>
<td>2015</td>
<td>342</td>
</tr>
<tr>
<td>Bank of Tokyo – Mitsubishi (Japan)</td>
<td>2014</td>
<td>315</td>
</tr>
<tr>
<td>Barclays (UK)</td>
<td>2010</td>
<td>298</td>
</tr>
<tr>
<td>Deutsche Bank (Germany)</td>
<td>2015</td>
<td>258</td>
</tr>
<tr>
<td>Bank of Tokyo – Mitsubishi (Japan)</td>
<td>2013</td>
<td>250</td>
</tr>
<tr>
<td>Clearstream (Luxembourg)</td>
<td>2014</td>
<td>152</td>
</tr>
<tr>
<td>Royal Bank of Scotland (UK)</td>
<td>2013</td>
<td>100</td>
</tr>
</tbody>
</table>


Figure 3
multiple channels and geographies, it is also more difficult to identify suspicious activities or gain a unified view of organization-wide risk.

The challenge for banks is to enhance their ability to detect, prevent and report financial crime while containing spiraling regulatory and compliance costs.

Six Steps to Fighting Financial Crimes

There is no silver bullet to preventing financial crime. Banks must take a series of steps to become more adept at fighting threats and navigating the complex regulatory landscape. Organizations can begin by conducting a comprehensive risk assessment, and then integrating the various financial crime prevention efforts across the organization to remove silos, improve the quality and availability of data, and create a culture of data-driven decision-making.

1. Tailor the Risk Management Approach

The key to developing and applying adequate controls is becoming knowledgeable about the risks themselves and the business areas they impact. A risk assessment should then be carried out based on the organization’s size, channels, geographies, customer types and product and service complexity (e.g., risks for wealth management products can arise from high-value transactions, politically connected individuals, multiple jurisdictions and banking secrecy). By mapping these risks against internal policies, procedures and controls, banks can assess their effectiveness in mitigating risks, and fine-tune them accordingly. A periodic review of the risk assessment should be conducted to ensure relevancy.

2. Address Silos

There is a wide spectrum of financial crime types, including money laundering, terrorist financing, fraud and cyberattacks. Intrusions, however, often go unnoticed, as these disciplines often operate in silos. To more effectively manage the growing sophistication of crimes, banks are increasingly focused on tightly integrating or merging the various internal functions tasked with financial crime prevention. However, some experts warn about the risks of such integration as it can increase vulnerability to cyberattacks, and instead recommend improving communication and coordination among the teams.⁵

We believe banks should start by integrating transaction monitoring in their cybercrime and AML disciplines to see the benefits for themselves, since these teams face similar types of challenges, and typically overlap in terms of processes, systems and data requirements. For example, if a cyber-attack occurs that involves the theft of online customer data, the team within the AML discipline could provide complete details of all suspicious activities flagged by its transaction monitoring systems. These details could then be used to cross-check any surge in e-commerce purchases, wire transfers, ATM withdrawals or similar transactions, thus detecting and preventing criminals from using the stolen data.

Similarly, a cyberattack alert by the cybersecurity team will enable the AML function to tighten transaction scrutiny and prevent money laundering, while the fraud prevention team can take steps to ensure the stolen customer data is not monetized, as well as investigate insider activity. The sooner the information is passed to the other teams, the more time they have to prevent the crime or identify the perpetrators.⁶

This type of collaboration will help banks gain new efficiencies in transaction monitoring and investigation, plug security gaps, reduce redundancies, streamline processes, innovate and build models that can identify and prevent even sophisticated crimes effectively, which can go a long way toward reducing costs and limiting financial damage.

3. Overcome Data Challenges

The key to integrating multiple risk efforts lies in the bank’s ability to get high-quality and consistent data from across the organization. This is no easy task for large banks, many of which have accumulated multiple systems and technologies over the years through mergers and acquisitions. Standardizing large volumes of customer, transaction, crime and other unstructured and semi-structured data from across the organization can be a challenge, as is encouraging employees to comply with internal standards and practices when entering data. However, doing so can significantly improve the overall data quality and accuracy needed to support real-time monitoring and data-driven decision-making.
4. Embrace Analytics
Combining effective data management with advanced analytics is essential for detecting and preventing growing threats. By collecting and analyzing the massive volumes of current and historical data within the organization (across all lines of business) and from external agencies providing financial crime data, banks can gain a comprehensive view of customers and transactions, as well as insights into relationships between various entities that previously went unnoticed. Through analytics, banks can better understand the risks posed by customers, transactions and other entities, and discover complex threats that impact multiple lines of business.

For instance, a transaction that appears legitimate in one channel may appear suspicious when viewed holistically. Forensic data analytics will help banks identify and predict risk patterns and issues in advance, enabling them to pre-empt criminal activity, particularly insider threats and data breaches that involve gaining unauthorized access to sensitive data.

5. Address Culture and People Challenges
The tone set by senior management is key to driving an organization’s crusade against financial crime. Senior bank officials need to set accountability standards, establish policies and controls, promote transparency by working closely with regulators, provide incentives for promoting compliance, and show zero tolerance toward potential internal and external risks.

Organizations should also grow their awareness of emerging threats, such as risks posed by virtual currencies and new channels and technologies. Employees should be trained and updated on the latest regulatory developments and emerging risks, and be sensitized to the various ways criminals can exploit them. High-risk users, such as contractors, suppliers and employees with access to sensitive organizational data and information, must be monitored and analyzed continuously for suspicious behavior or use of technology.

6. Collaborate with Industry-wide Initiatives
While banks have invested heavily to improve their compliance programs, evolving regulations have hindered them from developing a sustainable and scalable solution. Individual banks have developed proprietary solutions, with no industry-wide standards or best practices to guide them, resulting in duplicate efforts across the industry and accelerating compliance costs.

Banks need to move toward a more collaborative and unified approach, similar to what exists for international trade confirmation and settlement. Doing so would address skill shortages, facilitate the creation of standards and best practices and foster innovation.

By collaborating with law enforcement agencies and the government, banks can also take the fight against financial crime to the next level. A case in point is the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT) initiative, a one-year pilot started in February 2015 by the government, banks, law enforcement agencies and others. The task force, expected to become a permanent institution, was set up to study the scale and methods employed in money laundering, suggest remedial measures and improve intelligence-sharing across parties.

Looking Forward
Fast-evolving financial crime and regulatory uncertainty impacts banks of all sizes and warrants a proactive approach. Large banks with multiple lines of business must focus on integrating various crime prevention disciplines and building a culture that supports data-driven decision-making. Banks should consider hiring former military and law enforcement intelligence officers with expertise in analytics to proactively identify trends in transactions with links to terrorist organizations.

Small banks can seek technology and talent resources from businesses that specialize in cybercrime to avoid the high costs of procuring, maintaining and updating technology, as well as attracting and retaining people with needed skills, while also gaining the flexibility to offer new products and services and enter new business areas. This is significant as small banks are beginning to adopt new business lines or product segments that larger banks have exited due to higher BSA/AML compliance risks.

Improving collaboration within the banking industry, as well as with regulators and law enforcement agencies, will result in targeted efforts to prevent crime, improve compliance, alleviate talent constraints, contain costs and resolve other challenges.

A transaction that appears legitimate in one channel may appear suspicious when viewed holistically. Forensic data analytics will help banks identify and predict risk patterns and issues in advance.
References


Footnotes


About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process outsourcing services, dedicated to helping the world’s leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 100 development and delivery centers worldwide and approximately 233,000 employees as of March 31, 2016, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world.

Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.