HOW TO IMPROVE RELATIONAL EFFICIENCIES BETWEEN LAW ENFORCEMENT AND FINANCIAL SERVICES
INTRODUCTION

In today’s regulatory environment, financial institutions must be increasingly vigilant in the fight against money laundering. The recent Panama Papers debacle and other high-profile banking scandals highlight the plethora of threats posed by political corruption, terrorism financing and money laundering. Currency transaction reports (CTRs), which automatically report transactions of $10,000 or more, and suspicious activity reports (SARs), which flag irregular account activity, form the backbone of Bank Secrecy Act reporting and are financial institutions’ best assets in the enforcement of anti-money laundering (AML) policies.

The Federal Financial Institutions Examination Council defines the five key components of an effective SAR system as the following: identification, managing alerts, SAR decision making, SAR completion and continuous monitoring. But to properly install this foundation, financial institutions must transition away from “checkbox compliance,” or blind regulatory conformity, and customize risk-based AML systems.

In the aftermath of unprecedented financial sector reorganization, parent banks may have difficulty identifying risk due to the antiquated or divergent IT systems of their acquisitions. Additionally, poor information sharing, particularly with bank industry partners, hinders a holistic understanding of market threat patterns and high-risk clientele. Banks need to better coordinate compliance objectives with legal expectations by ensuring that they have designed clear and organized policies for interacting with regulators and law enforcement agencies. Collaborating with local, state and federal agencies can be confusing for financial institutions due to different reporting, monitoring and information-sharing demands.

The diversity of regulatory entities that may intersect financial crime investigations means that banks must have coordinated guidelines for multiagency and multijurisdictional compliance. Information sharing, with judicious data provisions, must become more fluid to identify criminality before it exposes banks to enhanced liabilities and fines. While collaborating with law enforcement can compound organizational pressures and disrupt normal bank operations, smarter engagement with law enforcement can mitigate financial crime and offer operational and cost-saving advantages to institutions.

Banks can improve relational efficiencies with law enforcement by customizing SAR reporting and monitoring to reflect their unique risk profiles. Additionally, institutions must update the IT databases of their subsidiaries to advance digital compliance continuity in the event of money-laundering probes. Other bank best practices for managing law enforcement relations include promoting know-your-customer (KYC) information sharing with partners and competitors and establishing clear policies, guidelines and compliance liaisons to help navigate investigations more intuitively.

While collaborating with law enforcement can compound organizational pressures and disrupt normal bank operations, smarter engagement with law enforcement can mitigate financial crime and offer operational and cost-saving advantages to institutions.
RISK-BASED SUSPICIOUS ACTIVITY REPORTS MONITORING AND REPORTING

Financial institutions face a diverse range of AML risk exposures, defined by size, customer demographics, geography, products and services offered and the wealth profile of their clients. AML monitoring systems are most responsive to transactional anomalies within various bank product silos. Standard bank product offerings are binary, limited to cash accounts and loans. Below are examples of common SAR flags for retail bank accounts and loan products.

CASH ACCOUNTS

- Structuring – multiple, small transactions to avoid CTR reports
- Round-dollar transactions – recurring exact transaction amounts
- Wires to and from high-risk jurisdictions (countries with weak rule of law, notoriety for organized crime, terrorism, political corruption, etc.)
- Activity profile deviations
- Dormant accounts

LOANS

- Early termination
- Multiple payments
- Third-party debt service

Additionally, globalization, technological disruption and regulatory scrutiny of large banks have reshaped patterns of illicit capital. Launderers, who may have previously sought a brand-name bank to custody criminal funds, may pivot towards an online institution to obscure the physical epicenter of criminal activity. Similarly, financial criminals may seek out relationships with smaller regional banks in non-urban jurisdictions that lack the monitoring controls of larger operators. While the digital revolution has liberated the flow of capital and enhanced the volume, velocity and complexity of transactions, retail banks still require in-branch presence for account opening and other transactions.

With this in mind, bankers are the first line of defense in identifying and reporting suspicious customers and account activity. But bankers must have suitable training, guidance and technology to spot the red flags that are most statistically relevant to their institution, product offerings and branch. Banks can better prepare their personnel to capture suspicious activity through the rigorous analysis of customer transactions and their internal SAR-filing history.

It is self-evident that every monitoring system needs to be based on the Bank Secrecy Act/anti-money laundering (BSA/AML) risk assessment – the mandatory compliance diagnostic that must be internally conducted by banks. But oftentimes, there is a disconnect between these monitoring systems and the unique risks that their enterprise users face. In fact, most AML rule scenarios focus solely on customer activity, without evaluating any of the bank’s KYC risks. In addition to compliance blind spots, these gaps also create excessive alerts, redundancies and false positives that can distract compliance analysts from true criminal threats.
Best practices to consider for improving SAR efficiencies include:

- Determine risk tolerances – business line, product, entity and geography
- Implement money-laundering risks identified in BSA/AML assessment into transaction-monitoring rules
- Train personnel to focus on unique risk categories and suspicious customer profiles/occupations
- Implement suppression logic rules to avoid alert redundancies for cases determined to be nonissues
- Perform quantitative assessment – statistical analysis to ensure rule thresholds are accurate and efficient
- Conduct periodic reassessment of monitoring rules to ensure systems are aligned with evolving threat environment

**UPGRADE SUBSIDIARY DATABASES**

In the wake of massive M&A activity in the financial sector, many larger banks have absorbed smaller community and regional operators domestically and abroad. These smaller institutions can pose significant compliance risks to their parent entities because their legacy data collection, record-keeping and monitoring systems may be primitive, disorganized or obsolete. With regulators holding parent banks more culpable for the compliance failures of their vendors, subsidiaries and other third parties, institutions must invest in the updating and standardization of databases throughout the bank.

By cleaning data, organizing records and normalizing record-keeping conventions to reflect parent company standards, banks can maintain the integrity of AML policies. An easily searchable and consistent IT framework simplifies law enforcement investigations and mitigates adverse outcomes down the road. The key is to be preemptive and avoid investigative business disruptions that can emerge from sloppy record keeping.

**PROMOTE INFORMATION SHARING**

In a sector notorious for its Machiavellian and anticompetitive practices, information sharing might seem the antithesis to the financial services operating model. Yet the growing sophistication of money launderers demands a united, industry-wide response. The United Kingdom’s Joint Money Laundering Intelligence Taskforce (JMLIT) is a prime example of the sector’s evolution towards collaboration.

Established in 2015 as a one-year pilot program, the JMLIT is an alliance between the British government, the British Bankers’ Association, law enforcement and more than 20 major banks under the leadership of the “Financial Sector Forum.” The task force believes information sharing will yield superior prioritization of risk, a more accurate and holistic view of emerging money-laundering threats, targeted intervention by law enforcement and greater opportunities to leverage interbank intelligence and best practices.

Banks in the U.S. and abroad should explore the British model and seek ways to share information without violating internal fiduciary or compliance policies. Through collaboration, banks can better achieve a multidimensional view of the money-laundering threat and identify criminal trends before institutional vulnerabilities get exploited.
CREATE MULTIAGENCY AND MULTIJURISDICTIONAL POLICIES AND GUIDELINES
There is no shortage of regulatory or law enforcement agencies that regularly interact with bank personnel. To mitigate confusion and organizational disruption, banks should establish clear policies and procedures for dealing with various federal and local entities. Compliance personnel must be aware of important regulatory and reporting deadlines, record-keeping expectations and key decision makers or liaisons for each of the different agencies. Additionally, compliance departments must designate key personnel to manage regulatory inquiries and law enforcement investigations.

Typically, these responsibilities will be delegated to the chief compliance officer. But in the event of multiple inquiries and investigations, the CCO would be wise to have competent lieutenants and officers ready to comply with investigative requests.

BEYOND SUSPICIOUS ACTIVITY REPORTS MONITORING AND REPORTING
In AML compliance, the old adage “the best offense is a good defense” continues to hold true. While these best practices for regulatory collaboration present significant advantages for banks in terms of transparency, efficiency and cost savings, the bulk of AML risk can be contained in the client on-boarding stage. Thomson Reuters CLEAR® records resource, a next-generation investigative software solution, has the capability to identify adverse customers and businesses before they threaten bank operations. In the digital age, technology is the thin red line separating institutional integrity from reputational ruin.

HOW THOMSON REUTERS CAN HELP
CLEAR online investigations software provides a solution to your compliance and investigative needs. CLEAR aids organizations like yours in mitigating financial crime by providing consistent, comprehensive and defensible investigative results.

For more on CLEAR and to request a free search and demo, visit: legalsolutions.thomsonreuters.com/law-products/solutions/clear-investigation-software