Current Challenges in Fighting Financial Crime
Since the economic downturn in 2008, keeping up with regulatory change has been a major challenge for most financial institutions, and for those operating in several jurisdictions or with multiple lines of business, the complexity increases exponentially. The regulatory landscape impacts many different business areas, including those involved in fighting financial crime such as anti-money laundering prevention, anti-fraud management and cybersecurity. Identifying exactly which regulation impacts which business area is a hugely complex task.

This multi-dimensional complexity impacts people, processes and technology in such a way that the current silo-based approach used by most major financial institutions in fighting financial crime is no longer sufficient. Ensuring compliance is a major challenge, while protecting the institution from cyber threats is becoming an even greater challenge. Both require a new compliance and security approach.
Why is compliance consuming such a high percentage of bank budgets?

There are a number of factors converging to make the fight against financial crime a major and costly challenge.

First, regulators around the world are all trying to solve similar issues. However, they all tackle them in different ways, with different rules. This means that, for regional or global banks with operations in several jurisdictions, the institution has to determine which rules apply to each transaction. The larger the institution and the more complex its operations, the more complex compliance becomes.

As an example, for sanctions screening, each jurisdiction issues its own lists of sanctioned entities, so checking each transaction in real time to ensure sanction controls are being properly followed requires several different black lists to be maintained, updated and used. Institutions need to know which lists to use for each transaction.

Second, the globalization of finance and the development of instantaneous electronic payment systems across multiple devices have had an unparalleled impact on the evolution of fraud. By the end of 2017, many countries will process transactions in real time (some even using a block chain, permissionless, distributed database protocol), so delinquent patterns will need to be detected within nanoseconds. Both trends also present considerable challenges for transaction monitoring, sanctions screening and customer due diligence.

In the banking world, this means that instead of checking and stopping transactions that are processed in a batch or overnight, everything now needs to be done in real time. So, if an alert is raised, it also needs to be checked immediately. This is driving up the cost of processing each alert.

Recent analyses estimate that each false positive alert costs a bank in excess of $30. With global banks processing millions of transactions and most dealing with false positive rates exceeding 5% of all alerts, the costs of managing alerts is becoming unsustainable.

Third, the threat of financial crime now includes financial fraud, money laundering and bribery, as well as a raft of new cybercrimes, which can be even more difficult to monitor and prevent. The threat has become so diversified that it is impossible for individual units or departments operating in silos to effectively manage it.
Across the globe, countries are moving to instant payments—building new infrastructures that enable SMEs and consumers to move money in real time from one account to another. In Europe, the new SEPA instant payment infrastructure will come into operation in 2017. Once fully operational, this will enable funds to be sent across borders in real time, creating another new business area that will need to be monitored. As these new schemes begin to communicate with one another, new areas of the bank will need to be monitored and require additional processing. At the same time, transaction volumes within traditional compliance areas are growing rapidly.

Both of these factors mean that more transactions will need to be scanned and monitored. As more transactions are scanned, more alerts will be produced and, therefore, more manual work will be required for rejecting or accepting the transactions, and the cost of managing compliance will continue to grow. As all transactions move to real time, the bank also has to manage alerts as they happen and cannot spread the workload out over time.

Due to new technologies, advanced, multi-dimensional cyber crimes have reached a level of sophistication that renders conventional law enforcement methods ineffective. Mitigating and responding to these new types of crimes will continue to be a problem, as predicting threats and new patterns is very challenging. The unprecedented scale of the problem threatens the ability of authorities to respond with, according to one estimate, more than 150,000 viruses and other types of malicious code in global circulation and more than 148,000 computers compromised per day.

On the other hand, authorities have more criminal activity data at their disposal than ever before, which greatly improves intelligence gathering and enables them to complete investigations in a more streamlined and cost-effective way.
Spotting the weaknesses helps to create opportunities

Analyzing fines issued by the Office of Foreign Assets Control (OFAC) in 2015 and the reasons for sanctions violations, in almost every case, the cause was an insider threat, such as the malicious use of credentials. While this is not the only cause, it is the main cause and a major issue. Therefore, most banks must address the issue and introduce much stronger cyber protection both externally and, more importantly, internally.

In implementing the best security practices, it helps not only to solve the core issue of protection for the institution, but also to promote that implementation across traditional and social media channels. As a result, client loyalty can be increased and market perception improved. Recent research has shown that protection of client assets is the highest priority issue for corporates and consumers when selecting a financial provider.

Clients are willing to leave their bank if their needs are not met and, conversely, if the bank meets their expectations, business will increase. A key weakness in most compliance strategies is the silo-based approach taken by institutions to fight financial crime and adhere to regulations. Historically, regulations that impacted corporate banking and those applied to retail banking were very different, so as the rules developed, strategies and processes were developed within specific departments in the bank. However, as digital transformation continues to accelerate and banking becomes real time, new payment solutions enable consumers to send funds cross border. Which rules should apply in this case? How does the institution fight against terrorist funding and prevent money laundering?

One answer to this is to begin breaking down the operational silos. By bringing together all alerts from across the bank, a single intelligent system can help the bank to spot noncompliance and stop suspicious activity. Pulling all alerts into one management environment would enable patterns to be spotted and help prevent potential additional fraud.

What about all the data the bank is processing? As financial and cyber criminals become ever more sophisticated in their attacks and approach to crime, the institution needs to develop new strategies to stay one step ahead. One answer to this lies in big data and artificial intelligence.

Most current systems used to detect suspicious activity in banks are based on rules. While these systems are fast and pick up most known issues, new crimes require constant review and regular updating of the rules to stay one step ahead. Artificial intelligence, on the other hand, is able to “learn” and provide valuable data that can be used to enhance protection. Recent CGI pilot projects in banks have shown that this big data approach to fighting financial crime can identify and track new crimes and uncover fraud currently undetected.
Summary

While we have only scratched the surface of the underlying issues most banks are tackling in their fight against financial crime, it is clear to all that the problem is getting bigger, and with the global trend toward real time, the costs for managing the alerts created is increasing.

The strategies discussed above may not be the complete answer, but if applied to most institutions, they would improve security, reduce compliance costs and increase client satisfaction.

One final point; banks need to find a way to educate their staff, customers and partners. To successfully fight financial crime, everyone needs to play their part. You can deploy the very best solutions in the world, but without due care and a concerted effort by everyone, criminals will continue to find a way to cheat the system.
Founded in 1976, CGI is one of the largest IT and business process services providers in the world, delivering high-quality business consulting, systems integration and managed services. With a deep commitment to providing innovative services and solutions, CGI has an industry-leading track record of delivering 95% of projects on time and within budget, aligning our teams with clients’ business strategies to achieve top-to-bottom line results.

www.cgi.com