THE GROWING THREAT OF MONEY LAUNDERING AS A SOPHISTICATED FINANCIAL CRIME

Organized crime and money laundering go hand in glove

Money laundering is big business – the United Nations Office on Drugs and Crime estimates that between 2 and 5 percent of the gross world product is laundered.

Money laundering is the processing of criminal proceeds to disguise their illegal origin. Most money resulting from criminal activity eventually enters the financial system. In many cases, a “legitimate” business is used as a front for laundering the proceeds of drugs deals or other crimes. Often criminals have several businesses to increase the complexity of money flows and reduce the chance of detection.

Consider the impact money laundering crimes had on a number of leading financial institutions in the past year alone:

- In early 2018, a major bank in India was featured in global news headlines for a conspiracy involving internal employees, a jeweler to the stars – and a fraud scheme that amounted to about $2 billion.
- In the fall of 2018, *The Guardian* reported that a top Nordic bank was being investigated for what would turn out to be a several years-long money laundering scheme estimated to have involved more than 6,000 customers. The bank’s stock price dropped more than 30 percent, and the CEO eventually resigned.
- About a month later, a tier one bank made news headlines when its headquarters were raided as part of a money laundering investigation.

It is widely believed that organized criminal gangs dominate money laundering. Why?

Money Laundering – A Global Industry

Success in money laundering calls for a complex infrastructure and scale that extends from the source of the illegal funds to the point of disbursement. In most cases, money passes through a three-stage cycle and it's crucial to understand each stage to improve prevention and detection:

1. **Placement of funds** into the financial system to dissociate from the original source of crime. This is the most likely way to catch criminals, as placing large sums of money into the financial system is likely to draw attention.

2. **Layering of transactions** to create a complex web of financial flows that thwarts detection. Money is moved through the financial system to break the audit trail and distance the money from the original crime. As the term laundering suggests, layering involves using the money for a range of legitimate purposes to ensure that it appears clean.

3. **Integration of money** to make it appear from a legitimate source. At this final stage, detection becomes more challenging as funds are integrated into the financial system and can be used for any legitimate purpose.

Are you doing enough?

Between 2012 and 2016 European banks were fined more than $16 billion for facilitating money laundering, according to Moody's Investor Service.[1] More than 75 percent of these fines were levied by United States regulators. In some cases, supervisors have offered banks deferred prosecutions in exchange for a period of extended regulatory oversight, during which they must improve their risk and regulatory oversight frameworks. These banks must work hard to reclaim their power and such events are a warning for all banks.

Most anti-money laundering (AML) regulations require the recipients of funds to exercise "reasonable care" as in any financial transaction. Banks and other financial institutions must exercise due diligence to ensure that they know their customers and the source of the funds.

The Financial Action Task Force (FATF) is an independent intergovernmental body that develops and promotes policies to protect the global financial system against money laundering.

FATF identifies some common "red flags" that might indicate money laundering:

- Frequent large cash transactions
- Use of large amounts of cash when checks would be expected and would be more convenient
- Frequent wire transfers to or from known bank secrecy havens around the world
- Immediate check or debit card withdrawals of large and frequent sums received by wire transfer
- An account holder who pays excessive attention to secrecy regarding personal or business identity
- Lack of general knowledge about the customer's stated business

[1]Moody's Investor Service, Sector In-depth, April 2019

The global rise of electronic payments and decline of cash use in most legitimate businesses is an aid to money laundering prevention but more must be done. Although there is a large and growing body of AML legislation, much of this is very high level and criminals can exploit gaps. Financial institutions must do more to detect money laundering activity.

Three Things Banks Can Do to Detect Money Laundering

1. **Recognize money laundering as a business challenge.** Financial crime prevention and detection must be the concern of all stakeholders and part of the firm's culture. Everyone should be aware that financial crime is a major threat to brand and reputation.

2. **Understand the money laundering cycle.** All staff must be able to identify the risks faced at each stage. Specific risks will vary from country to country, depending on the types of crime that are prevalent in the specific geography. Once specific risks are identified, these should be incorporated into the AML compliance framework and reviewed periodically.

3. **Use technology to boost surveillance.** Soaring transaction volumes provide new ways to launder money. Modern AML intelligence solutions can be deployed at the enterprise level to monitor customer behavior, identify irregular transactions and detect when theft or account takeover seems likely.

FIS Memento: Outsmart your enemy

FIS Memento is the industry's leading enterprise-wide, schema-agnostic fraud management tool that knows what your enemies will try, before they do. It predicts financial crimes in every channel to put the power back in your hands. With highly scalable machine learning and AI capabilities, FIS Memento spots fraudulent transactions across your entire firm in real time, predicts new threats and offers the cross-channel tools your staff needs to efficiently and holistically manage any threat. FIS has ranked No. 1 on the RiskTech100 list four years running for a reason.

TO LEARN MORE ABOUT FIS' INNOVATIVE FINANCIAL CRIME MANAGEMENT SOLUTIONS, click here OR CONTACT getinfo@fisglobal.com.