REUTERS

CREDIT RSS

MARCH 14, 2018 / 9:15 AM / 2 YEARS AGO

Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states

Joshua Fruth

NEW YORK (Thomson Reuters Regulatory Intelligence) - Regulators are holding financial institutions responsible for the real-life consequences of anti-money laundering (AML) failures. Firms must reconfigure their transaction monitoring programs to identify the emergent, multi-dimensional money laundering and terrorism finance methods that are defeating today's rules-based detection scenarios. Adopting an actor-centric hybrid threat finance (HTF) model can cut compliance costs, reduce risk, improve regulatory relations, and increase the usefulness of suspicious activity reports (SARs).

A pedestrian looks over at masked, and heavily armed, Mexican Federal agents as they stand guard, June 21, 2001, outside a Mexican money changing house during raids on properties in the capital linked to yesterday's DEA "Operation Marquis" in which tons of narcotics and over two hundred suspects were arrested in an attempt to close down a large cocaine smuggling operation allegedly linked to the Juarez cartel.

Financial institutions are required by the Bank Secrecy Act (BSA) to detect and report customers engaged in money laundering, fraud, terrorist financing, and sanctions violations. With millions of customers, banks have fielded automated transaction monitoring systems, which use money laundering detection scenarios known as rules, to alert firms to certain customers for potential violations. Current industry detection logic has proven flawed and inefficient at identifying financial crime, resulting in record-breaking regulatory fines for financial institutions that fail to detect terrorists, drug cartels, and sanctioned state actors exploiting the U.S. financial system.

BANKS FOCUSED ON SIMPLE TRANSACTIONAL BEHAVIORS

Banks have spent billions on transaction monitoring systems that scrub their accounts for possible money laundering schemes. Detection rules are action-based and target suspicious transaction behaviors, such as excessive cash deposits, structured transactions intended to avoid government record-keeping thresholds, and rapid money movement through one bank to another.

Customers who violate the detection rules trigger a system-generated alert, which is reviewed by an internal investigator. Despite decades and billions of dollars in industry investment, over 95 percent of system-generated alerts are closed as “false positives” in the first phase of review, with approximately 98 percent of alerts never culminating in a suspicious activity report (SAR).

False positives cost the financial industry billions of dollars in wasted investigation time each year but more importantly, expose banks to steep fines and reputational damage for failing to identify bad actors involved in organized crime, sanctions evasion, or terrorism. Banks can reduce risk by reassessing their detection strategies, which presently lack the focus or sophistication to identify illicit source behavior.

REGULATORS AND LAW ENFORCEMENT AGENCIES FOCUSED ON THREAT ACTORS

Unlike fraud, money laundering stems from a precursor criminal act, like extortion, misappropriation of funds, or trafficking. As such, most global money laundering is perpetrated by transnational criminal organizations (TCOs), rather than individuals. Bank accounts used to launder illicit proceeds may be set up for personal or business use, but are most often used to cleanse funds on behalf of a threat organization. As one might imagine, different threat groups launder money in different ways.

For this reason, law enforcement agencies (unlike banks) target money laundering purpose; meaning they consider both source criminal behavior (e.g. drug trafficking) and illicit organizational membership. When a U.S. law enforcement investigation into a crime syndicate or terrorist group identifies suspect bank accounts, the Treasury Department’s Financial Crimes Enforcement Network (FinCEN) issues request for information notices (known as 314(a) forms) to those banks. The resulting case investigations often reveal that banks failed to detect or investigate these suspicious accounts, leading to increased regulatory scrutiny that opens the floodgates to fines and remediation.

THE TOTAL COST OF FAILURE

When bank AML programs neglect detection considerations for money laundering purpose and preceding illicit activities, they fail to identify bad actors exploiting the firm. Such failures have caused major institutions to incur hundreds of millions, or billions, in regulatory penalties and associated costs. Global and retail banks, money service businesses (MSB), digital currency exchanges, and casinos are all at risk of crushing enforcement actions. Financial institutions globally have been fined over $321 billion by regulators since 2008 (PDF) (here), with $42 billion in fines in 2016 alone.

The monetary penalty value, according to a McKinsey & Company analysis dating back to 2005, turns out to be the lesser issue when compared with the following:

—A regulatory fine is a top-five loss event for any bank (alongside embezzlement, loan fraud, revelations of deceptive sales practices, and anti-trust settlements);

— Corporate share values decline approximately 6 percent the day fines are announced;

— Cease and desist orders result in loss of new programs, vendors, and business plans;

— Remediation costs over the first 18 months are typically 12 times greater than the fine itself.

Firms incur not only financial loss, but also reputational harm. Regulatory enforcement actions often feature specific language indicating that banks aided and abetted terrorism, drug trafficking, and human trafficking by failing to detect and report illicit activity. Financial institutions have learned the hard way that regulators hold them responsible for the broader outcome of AML failures, not just their program's procedures. Additionally, media outlets are quick to capitalize on negative news about large corporations, which can trigger a public relations disaster, especially when amplified by viral social media.

FAILED APPROACHES TO REMEDIATION

When a regulatory fine is enforced upon a bank, it is often accompanied by a consent order requiring a forensic (lookback) examination of customer data to identify previously undetected risks and suspicious activity. This often results in tens of thousands (or more) of

historical transaction-monitoring alerts that need to be reviewed in tandem with current alert output. As a result, many banks hire external consulting firms to address the alert backlog, which can end up costing many times more than the regulatory fine itself.

Many of these same consulting firms market AML detection products and services that claim to reduce false positives and improve SAR filing percentages. For retail banks, these firms focus on tuning the very action-based rules that failed in the first place, without providing new scoring tables or custom data attributes to improve performance. In global correspondent banks, the detection rules are even less focused, due to limited information on external parties (i.e., non-customers) conducting global wire transfers.

More expensive providers market high-tech applications, like unsupervised machine learning (UML) and artificial intelligence (AI) software, billed as a turnkey solution that updates scenarios based on quantitative abnormalities that lack common-sense detection logic. These applications are largely developed by technical specialists such as computer scientists who are unlikely to possess the requisite law enforcement, intelligence, and financial crime backgrounds to effectively target emergent risks.

AML detection is a dynamic process that requires awareness and consideration of transnational security issues, public policy, and the regulatory climate – areas simply not being calculated into these AI scenarios. While UML/AI software improves efficiency in many business areas by instantly siphoning through vast quantities of structured and unstructured data, the complexities of money laundering tradecraft means there can be no magic bullet for solving detection challenges.

Keep in mind: AML detection is already automated, just not predictive. Transnational criminal organizations employ professional money laundering cells that do not operate within the confines of expected, predefined, overly-broad transactional actions. Firms that continue to focus their detection strategies on UML/AI software and broad action-based targeting will fail to identify emergent threats and risk the ire of regulatory agencies.

HEZBOLLAH AS HYBRID THREAT FINANCE EXAMPLE

Criminal cartels, hostile states, and terrorist groups today form hybrid threat alliances that extend through their finances. In some cases, one single group may be classified as a hybrid threat organization. The Lebanese Shiite Islamic group Hezbollah is one such example.

Designated by the U.S. State Department as a terrorist organization, Hezbollah is aligned with the Iranian Islamic Revolutionary Guard Corps (IRGC), Palestinian Hamas, Yemen's Houthi rebels, and nearly one-hundred Shiite militant groups in Iraq, Syria, Afghanistan, and elswehere. These connected Shiite militant groups (Hamas is Sunni) collectively report to Iranian Supreme Leader Ali Khamenei. Iran is subject to a number of U.S. and international economic sanctions.

Hezbollah has recently become a hot-ticket political issue for U.S. Attorney General Jeff Sessions, who in January 2018 announced the Hezbollah Financing and Narcoterrorism Team (HTNT) (here), an interagency team of prosecutors and investigators tasked with targeting Hezbollah's criminal and money laundering networks. This announcement followed revelations outlined in a media report alleging the Obama administration derailed a Drug Enforcement Administration (DEA) program targeting Hezbollah's trafficking operations (here), in order to secure the 2015 Iran nuclear deal (here).

Sessions has indicated (here) that targeting Hezbollah's money laundering operations will be a primary focus of the current administration; an emphasis set to extend to bank regulators.

According to a December 2016 terrorism finance report (PDF) (here) by the U.S. House of Representatives Financial Services Committee, Hezbollah is a hybrid threat organization with a global footprint. With a structure that includes a Lebanese political party, conventional military, Iranian terrorist proxy force, and crime syndicate, Hezbollah is one of the world's most unique and versatile threat groups.

Hezbollah's crime syndicate is extremely multi-faceted, with long-held narcotics, human trafficking, and counterfeit goods underworld networks throughout the tri-border Area of Latin America, the Middle East, North/West Africa, and Asia.

Hezbollah maintains one of the most sophisticated and efficient trade-based money laundering (TBML) operations in the world, as evidenced by the 2012 Lebanese Canadian Bank

laundering case (PDF) (bit.ly/2FCTV6h). Their TBML tradecraft is so proficient that they hide drugs and cleanse narcotics proceeds by owning all parts of an elaborate global distribution network that falsifies the number of shipments and amount of products shipped, while concurrently hiding counterfeit goods among legitimate products (here).

This double-dipping smuggling and false invoicing operation provides the profit margin Hezbollah needs to purchase weapons, tactical kit, and to provide logistical support to their global insurgency operations in places like Iraq (here), Syria (here), and Yemen (here).

Hezbollah's business and money laundering tactics are extremely specific and unique (compared to other groups) and require seasoned intelligence practitioners to identify. They use virtually all banking products, including international wires, retail services, prepaid products, and money service businesses (MSBs) at different operational echelons, ranging from international/strategic to regional, domestic support companies (DSC), and at the tactical level.

Accordingly, this one organization presents separate enforcement and reputational risks at different levels of operation.

Like Hezbollah, other militant groups, drug trafficking organizations (DTOs), human trafficking outfits, and hostile nation-state actors are also competent money launderers. They too possess a hierarchical, multi-echelon global structure that utilizes numerous controls designed to subvert modern AML detection mechanisms. These groups hire professional money launderers with a detailed knowledge of compliance that could rival the AML experts working at banks.

Professional money launderers working for global threat organizations launder funds in ways that superficially appear entirely legitimate, failing to raise red flags through conventional detection strategies. Put simply, these professional criminals are unlikely to make amateur mistakes, such as structuring or rapid withdrawal of cash.

FLAWED APPROACH

Detection logic focused on simple transactional behavior will never successfully identify money laundering operations by sophisticated hybrid threats like Hezbollah. Banks might think unsupervised machine learning (UML) and artificial intelligence (AI) software sounds new and exciting, but these programs detect anomalies and mistakes that professional money launderers are unlikely to make.

HYBRID THREAT FINANCE DOCTRINE

The best way to address these challenges is with a detection platform based on the hybrid threat finance (HTF) concept derived from the U.S. Department of Defense "hybrid threat" doctrine. The military, intelligence, and law enforcement communities recognize the hybrid nature of international conflict relations, in that threat organizations across different classifications are deeply interconnected. HTF methodology targets the extension of those connections into financial markets, focusing detection strategies on the fund flows and intersections between one or more threat groups or operational echelons in international and retail banking, gaming, MSBs, and digital currency exchanges.

Institutions should adopt an "actor-centric" HTF model that targets bad actors with precision, increasing SAR efficacy rates and decreasing false-positive alerts. This concept relies heavily on a typology matrix, which analyzes a bank's geographic nexus of services, products, and customer base, while cross-referencing identified risks in the global threat landscape. Matches between geography, product line, and high-risk customer profile are tied to specific threats, which leads to the implementation of targeted detection scenarios.

Additionally, it is incumbent upon banks to also train their investigations, sanctions, and risk personnel in these new detection scenarios. Sound detection strategies are of little value if the people investigating the behavior lack the requisite knowledge to identify and escalate threat activity.

CONCLUSION

The New York Department of Financial Services (NYDFS) in 2017 implemented new bank transaction monitoring requirements (Part 504) (PDF) (here), which redefined SARs to include the following language: "identifies suspicious or potentially suspicious or illegal activities". This is in stark contrast to past regulatory language that called for the identification of suspicious "transactions".

Regulators are holding financial institutions responsible for the outcomes of compliance failures, not just their processes. AML units who update their detection logic to a hybrid threat finance model stand to cut costs, reduce risk, improve regulatory relations, and provide improved financial intelligence products to law enforcement, intelligence, and military officials keeping our nation safe.

Joshua Fruth is the Director of anti-money laundering advisory services at New Jersey based consultancy Matrix-IFS www.matrix-ifs.com/. The views expressed are his own.

MORE FROM REUTERS

Britain's Prince Harry: 'I will not be bullied into playing a game...

21 Oct

China says will not change position on Taiwan after landslide election

12 Jan

'Disastrous mistake': Iran acknowledges shooting down Ukrainian...

12 Jan

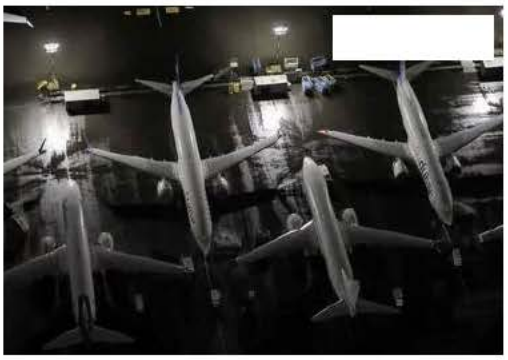
U.S. winter storms cause 10 deaths, flight cancellations, power...

12 Jan

'I'm spending all my money to get rid of Trump': Michael Bloomberg

12 Jan

MORE FROM REUTERS



'Designed by clowns': Boeing employees ridicule 737 MAX, regulators...

11 Jan

U.S., China agree to semi-annual talks aimed at reforms, resolving...

11 Jan

Small but dangerous: volcano spews ash over Philippine capital

12 Jan

Factbox: Reactions to Iran's statement it downed Ukrainian plane

11 Jan

Canada's Trudeau wins plaudits at home as Iran admits causing crash

12 Jan