REGULATORY INTELLIGENCE BRIEFING — ISSUE 8, 2018

MONEY LAUNDERING:
TOP TRENDS AND HOW TO PROTECT YOUR INSTITUTION

Capco Center of Regulatory Intelligence

CAPCO

IN THIS ISSUE

EDITORIAL NOTE FROM THE MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE

PETER D. DUGAS
MANAGING PRINCIPAL, CENTER OF REGULATORY INTELLIGENCE

Peter has more than 16 years of government and consulting experience in advising clients on supervisory matters before the U.S. government and in the implementation of enterprise risk management programs. He is a thought leader in government affairs and regulatory strategies in support of banks' and financial institutions' compliance with the Dodd-Frank Act and Basel Accords. Prior to joining Capco, he served as a director of government relations at Clark Hill and in senior government positions, including serving as a deputy assistant secretary at the United States Department of the Treasury.

Effective anti-money laundering (AML) programs are one of the cornerstones of every institution's risk governance. Over the years, money laundering techniques have become more complex and difficult to detect. The systems set in place to raise red flags for suspicious activity are an institution's best resources in combatting money laundering threats, and it is critical to ensure that these systems are functioning appropriately and effectively.

This month, Capco Center of Regulatory Intelligence (CRI) tackles some of the most topical risks in AML compliance, and provides examples of actionable best practices through systems testing.

We examine professional money laundering, using the recent paper the Financial Action Task Force (FATF) published on the issue as a blueprint for discussion. Then, we look at current trends in threat finance, covering the most pressing questions for the C-suite in this area. Finally, we deliver a snapshot of how the opioid crisis has affected financial institutions, and what the warning signs may be for the illegal financial activity associated with this health epidemic.

The second half of our spotlight article focuses on proactive anti-money laundering (AML) efforts, specifically outlining three levels of transaction monitoring system testing. The three distinct levels of testing illustrate unique levels of comprehensiveness, and are meant to show how an institution can best protect itself based on the institution's specific risk appetite and applicable regulatory requirements.

Our secondary article this month delves into the complexities of marketing via social networking websites and platforms. Just this month, a leading social media-based company found itself the subject of a formal complaint from the U.S. Department of Housing and Urban Development (HUD). While this particular legal investigation places the onus of compliance on the website itself, the complaint emphasizes the need for financial institutions to fully understand the regulations for social media marketing.

Other recent enforcement actions highlight the repercussions on financial institutions for misusing social media in business practices, and especially for marketing efforts. Our article offers insight into what institutions should pay specific attention if they decide to advertise their products and services on social networking platforms.

As always, Capco continues to monitor these and other areas impacting financial institutions' risk and compliance functions. If you have any questions regarding how to garner further information on these topics, please reach out to us at capco.cri@capco.com. ❖

REGULATORY ROUNDUP

Regulatory and Compliance Alerts

FDIC Updates SOP regarding Bank Hiring Practices

On August 3, 2018, the Federal Deposit Insurance Corporation (FDIC) updated its Statement of Policy (SOP) related to section 19 of the Federal Deposit Insurance Act. Section 19 prohibits, without the prior written consent of the FDIC, any person from participating in banking who has been convicted of a crime of dishonesty or breach of trust or money laundering, or who has entered a pretrial diversion or similar program in connection with the prosecution for such an offense. The final statement of policy was applicable starting July 19, 2018.

CSBS Announces Nationwide Adoption of Single Exam for Mortgage Licensing

On August 8, 2018, the Conference of State Bank Supervisors (CSBS) announced that all states and U.S. territories now use a single, common exam to assess mortgage loan originators (MLOs), simplifying the licensing process for MLOs and streamlining supervision of the mortgage industry.

CFPB Issues Final Rule on Regulation P

On August 10, 2018, the Bureau of Consumer Financial Protection (BCFP or CFPB) finalized amendments to Regulation P (Gramm-Leach-Bliley Act) to implement legislation that allows financial institutions that meet certain requirements to be exempt from sending annual privacy notices to their customers. **The rule is effective 30 days after publication in the Federal Register.**

HUD Issues ANPR on Fair Housing Regulations

On August 13, 2018, the Department of Housing and Urban Development (HUD) issued an Advance Notice of Proposed Rulemaking (ANPR) related to amendments to HUD's "Affirmatively Furthering Fair Housing" (AFFH) regulations. **Comments are due within 60 days of publication in the Federal Register.**

SEC Adopts Amendments to Simplify and Update Disclosure Requirements

On August 17, 2018, the Securities and Exchange Commission (SEC) adopted amendments to eliminate redundant, overlapping, outdated or superseded provisions, in light of other SEC disclosure requirements, U.S. Generally Accepted Accounting Principles (GAAP), International Financial Reporting Standards (IFRS) and technology. **The updates are effective 30 days after publication in the Federal Register.**

Agencies Issue Interim Final Rule on Liquidity Coverage Ratio

On August 22, 2018, the FDIC, Federal Reserve Board (FRB) and Office of the Comptroller of the Currency (OCC) issued an interim final rule to amend the agencies' liquidity coverage ratio rule to treat liquid and readily-marketable, investment grade municipal obligations as high-quality liquid assets. **The rule is effective upon publication in the Federal Register, and comments will be accepted for 30 days.**

MONEY LAUNDERING:

TOP TRENDS AND HOW TO PROTECT YOUR INSTITUTION

TRENDING AML THREATS

The United Nations Office on Drugs and Crime estimates that illicit cash flows account for 2 – 5 percent of the global GDP, amounting to $800 billion to $2 trillion per year. Financial institutions are increasingly aware of the ways their organizations may unwittingly play a part in this statistic, and the implications of faulty safeguarding, both to their individual institutions and to the financial system as a whole.

The idea of combatting money laundering is not a new one, and every financial institution likely has a system in place to comply with applicable laws and regulations. Within the last few years, institutions have seen shifts in certain aspects of their anti-money laundering (AML) programs, including the swift progression of technology and the risks posed through cybersecurity and virtual currencies; new requirements for beneficial ownership identification; and periodic updates to sanctions lists.

However, as AML trends continue to develop, institutions are sometimes so focused on the tangible new legal obligations and compliance requirements that identifying and tracking new trends is overlooked. In this article, we highlight three areas of money laundering risk that have seen a rise in visibility in recent years, and what the implications are for proactive, forward-looking AML programs. We end the article with some suggestions for hands-on best practices, to ensure institutions can evaluate whether they have the tools in place to combat these trending threats.

A QUICK BACKGROUND ON AML AND RELATED LAWS AND REGULATIONS

1970 The Bank Secrecy Act (BSA) passes into law, including provisions on reporting requirements, such as the Currency Transaction Report (CTR), intended to help law enforcement find proceeds derived from illegal activities, primarily drug trafficking. In an effort to remain anonymous, most criminals conduct illegal transactions with cash, which is harder to trace than other forms of payment. CTRs were designed primarily to catch the placement of illicit cash into the financial system.

1986 The Money Laundering Control Act passes into law, making money laundering a federal crime.

1994 The Annunzio-Wylie Money Laundering Suppression Act passes with requirements for Suspicious Activity Reports (SARs). This makes financial institutions responsible for reporting activity that they suspect is intended to conceal the source of funds that may be in violation of the BSA, such as structuring transactions to avoid CTR filing. SARs help law enforcement detect money laundering both when illicit funds are placed back into the financial system and in the concealment phase.

1990 Financial Crimes Enforcement Network (FinCEN) is created under the Department of the Treasury (Treasury). Established as the financial intelligence unit (FIU) for the U.S., "Its original mission was to provide a government-wide, multi-source intelligence and analytical network to support the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes." Today, FinCEN still acts as intermediary between financial institutions and law enforcement, by maintaining databases of CTRs and SARs.

2001 After the terrorist attacks on September 11, 2001, the USA PATRIOT Act enacts twelve specific sections focusing on preventing and detecting international money laundering and shell banks that serve as fronts in money laundering on behalf of terrorist financing.

TRENDING AREA ONE: PROFESSIONAL MONEY LAUNDERING

On July 26, 2018, the Financial Action Task Force (FATF) issued a report on professional money launderers (PMLs) — third-party individuals, organizations or networks who, for a fee or commission, specialize in enabling criminals to evade AML and counter terrorist financing (CTF) safeguards and sanctions in order to realize profits from illegal activities. The report aimed to help countries identify and dismantle these professionals by looking at the key characteristics, tools and techniques PMLs use to engage in this business.

What Are PMLs?

- PMLs profit from revenue-generating criminal activity, but are not engaged in the predicating, revenue-generating crime.
- They act as experts to move illicit funds without detection, concealing the nature, source, location, ownership, control, origin and/or destination of funds to avoid detection.
- The models for such laundering initiatives can be full and complex in scope, or tailored to an individual activity; PMLs can be involved in one step or the entirety of the money laundering process for each engagement.
- PMLs provide a list of services, and often do not differentiate between the different types of crimes from which the funds in question were derived.

How do PMLs Operate?

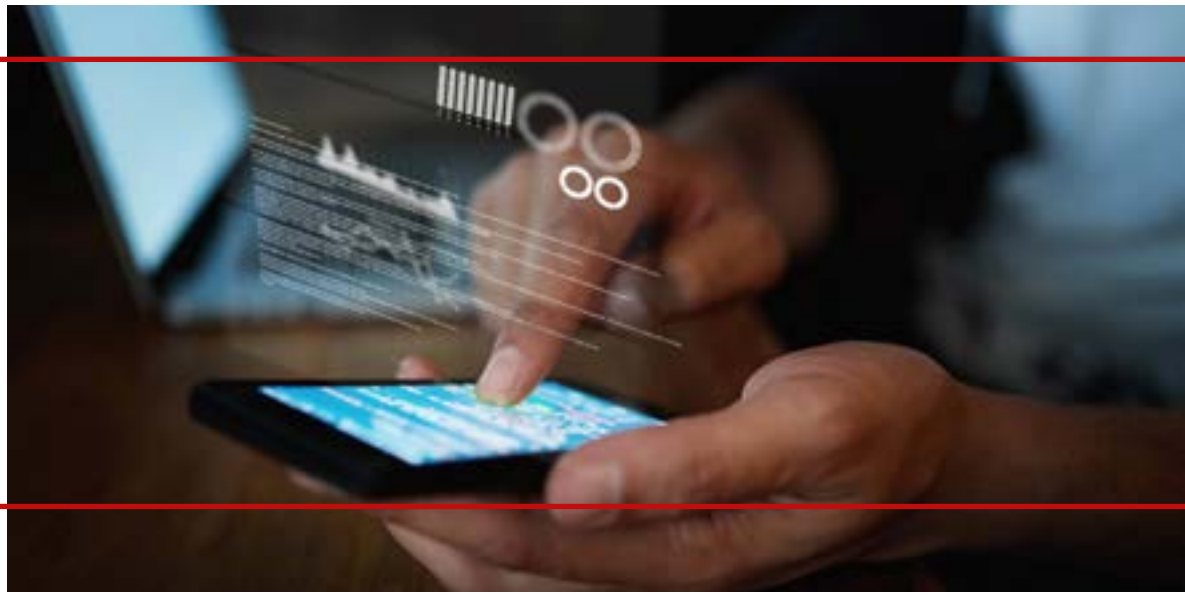
- PMLs generate their customer base primarily through word-of-mouth, though there is also evidence of advertising efforts on the Dark Web.
- PMLs charge for their services by taking cash in advance, transferring a portion of the illicit funds to the PML's own account or integrating commission into the transaction itself.
- Generally, there are three steps to a PML's services: collecting the criminal proceeds, layering the funds to convolute streamlines and returning the laundered funds to clients for investment or asset acquisition.
- There are four main types of PMLs: money transport and cash controller networks; money mule networks; digital money and virtual currency networks; and proxy networks.
- An individual PML's tactics can overlap between clients, and multiple organized criminal groups' funds might therefore utilize the same channels for certain steps of the money laundering cycle.

What Are Some Methods PMLs Use?

/ **Trade-based money laundering:** In "trade-based money laundering" (TBML), bad actors can interact with the financial system through seemingly legitimate businesses, often choosing high-risk markets such as precious metals. By misrepresenting the value, quantity or quality of goods, it is then possible to exploit the international trade system, hiding the true sources of funds and transferring funds across international borders. These models can range from simple to highly complex, but they continue to scale up as the global trade market grows. For example, PMLs can purchase high-value goods with criminal proceeds and re-sell the goods overseas; falsify the number or value of goods being shipped; or use money brokers.

/ **Account settlement:** Because the PML is providing services to criminals who have cash that they need to disperse and other criminal groups which need cash to pay their networks and workers, the PML can provide an account settlement mechanism and make a profit in the process.

/ **Underground banking:** Used to bypass regulated financial institutions, this could use a medium of exchange such as casino chips or alternative banking platforms (a form of shadow banking that uses some services of a formal banking system, but has its own parallel accounting and settlement system with the backbone of custom transactional software).



What Risks do PMLs Pose?

- PMLs often operate on a large scale and across international borders.
- Many countries do not have sufficient programs in place to detect third-party laundering activity, and many countries limit prosecutorial action to first-party criminals, making it difficult to take down PMLs.
- The actors themselves often have no criminal background, and sometimes come from professional and legitimate backgrounds. They are therefore harder to detect, as they are unlikely to show up in searches and are well-trained and experienced.
- Compartmentalized organization structures and relationships can mean there are several degrees of separation, and therefore traceability, between those in charge of the funds-generating activity and the masterminds behind the laundering. This means that even if a PML is detected, the criminal groups it supports may still be protected, and vice versa.
- PMLs are too smart to use only one bank; therefore, a single institution, at best, is only going to detect one small part of the overall operation.

Detecting and Deterring PMLs

Depending on how the PML uses domestic and international wire transfers, a suspicious activity rule which analyzes originator and beneficiary names for "many to one" transactions could detect a part of the scheme. Additionally, the companies perpetuating money laundering activities would likely receive funds from seemingly unrelated businesses which don't connect with the supposed purpose of the main business. It seems that the best way to fight these operations would be to have a focused national-level law enforcement and supervisory action, in addition to appropriate regulation, cooperation and information exchange internationally.

The FATF report dives into the specific structures of PML networks, types of tactics PMLs use, examples of PML activities, tools and techniques PMLs utilize, types of actors involved in PML initiatives and areas where PML usage is prevalent, but does not discuss combatting PMLs. However, FATF also created a non-public version of the report (for Members of the FATF and the FATF Global Network) to provide recommendations for the detection, investigation, prosecution and prevention of PML activity. We may begin to see examples of how these recommendations are utilized in the near future.

Looking forward, Capco CRI believes this will continue to be a trending issue on a global level, and it seems likely that more government agencies will publish additional information and guidance on the subject, to highlight functions that may deter this unique criminal activity.

TRENDING AREA TWO: THREAT FINANCE

Threat finance — the methods and tactics organizations use to fund activities that threaten national and international security — continues to be a major concern, both globally and in the US. This type of money laundering disguises large proceeds from serious crimes as legitimate so that they can be used by actors such as:

- International terrorist organizations
- Drug cartels/narcotics traffickers
- Transnational organized crime groups
- Arms traffickers
- Wildlife traffickers
- Cybercriminals
- Identity-related criminals
- Organ traffickers
- Illegal mining operations
- Pirates
- Counterfeiters

Among the largest issues in combatting threat finance are the low barriers to trade and movement of capital on a global level, as well as technological innovations that make it almost impossible to detect and obstruct illicit operations.

There are overlaps in the methods threat finance uses and the methods PMLs and other types of money laundering utilize. Some methods of threat finance include:

- Trade-based money laundering (TBML)
- Real estate
- Gambling junkets
- Mining
- Digital currencies
- Phishing
- Online gambling
- Dark markets
- Ransomware
- Online advertisement fraud

Threat finance protections are constantly changing as high-level intelligence units monitor global risks. For example, the Office of Foreign Assets Control (OFAC) regularly updates its sanctions lists in response to a variety of intel on bad actors and potential threats. Some recent additions to these lists include:

/ **August 21:** OFAC designated two Russian entities and six Russian vessels involved in the ship-to-ship transfer of refined petroleum products with North Korea-flagged vessels, an activity expressly prohibited by the United Nations Security Council (UNSC).

/ **August 21:** OFAC designated two entities and two Russian individuals based on the actions they undertook for Divetechnoservices, a Russian entity sanctioned on June 11, 2018 (for procuring a variety of underwater equipment and diving systems for Russian government agencies, to include the Federal Security Service (FSB), itself sanctioned in March 2018).

/ **July 31:** OFAC designated two individuals (financial facilitators) for acting for or on behalf of Lashkar-e Tayyiba, a terrorist organization based in Pakistan.

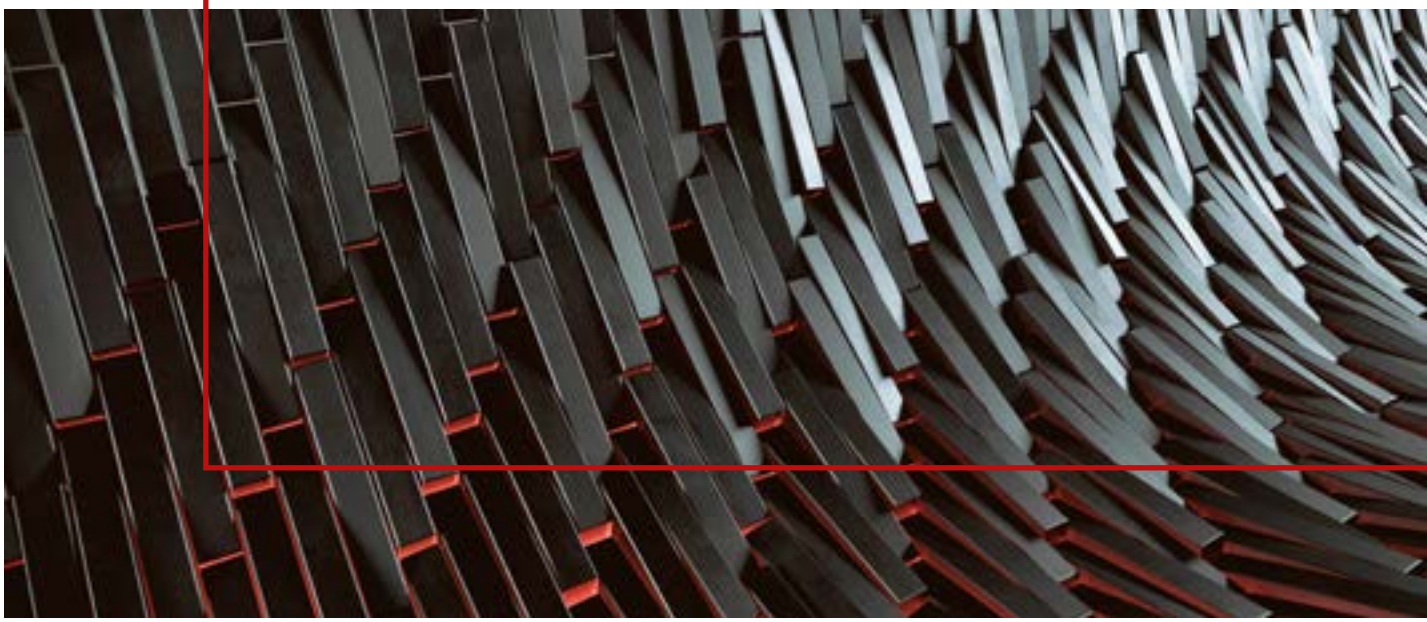
/ **July 25:** OFAC designated five entities and eight individuals, who are key components of a vast network procuring electronics on behalf of Syria's Scientific Studies and Research Center (SSRC), the agency responsible for the development of Syria's chemical weapons.

In addition to keeping track of these lists and staying abreast of urgent alerts, the C-level suite continues to have concerns regarding threat finance. In recent interviews with top executives of financial services institutions, some of the common themes in relation to threat finance revolved around the idea that technology today is both the most advanced and complex it has ever been, and it continues to evolve rapidly.

The positive side of this is that available safeguards are increasingly powerful, and the potential for collaboration, aided by technological innovations, leads to an interconnectedness that is critical to combatting threat finance. But, as financial institutions become better at predicting, detecting and preventing threat financing efforts, bad actors also become more sophisticated.

It has become best practice, therefore, to no longer use a 'check box' approach to financial crime safeguarding and compliance. It is essential that financial institutions have the ability to effectively demonstrate that their AML/CTF systems are working against specific types of threats.

In the Best Practices section at the end of this article, Capco will provide some ideas for a more integrated and thorough system to better protect institutions and their communities.



TRENDING AREA THREE: THE OPIOID EPIDEMIC

In 2017, FinCEN gave New York State Police an award for identifying over 100 individuals involved in a large illegal operation after a single financial institution reported an unusual pattern of cash deposits. After funds were rapidly withdrawn from ATM locations across the U.S., the reporting bank indicated that it believed much of the cash was derived from the illegal sale of marijuana. Investigations led to the discovery of a huge amount of cash stored up from the sale of illegal opioids, and the single financial institution responsible for reporting its suspicions helped New York State Police make the discovery that busted this dangerous criminal group.

Some other recent instances of money laundering involve the illegal practices around distribution of legal drugs. This is arguably more difficult to detect than the distribution of unlawful drugs, even though unlawful drug sales present a challenge of often being cash-based. When someone has a license to prescribe opioids that are legal, but they abuse it by overprescribing or prescribing them unnecessarily, it can be much more difficult to distinguish a legal transaction from an illegal one.

In 2017, the operator of a pharmaceutical company was arrested for bribing doctors to prescribe legal opioids to their patients unnecessarily. The indictment also alleged that the company conspired to mislead and defraud health insurance providers who were reluctant to approve payment for the drug when it was prescribed for non-cancer patients.

In another case in 2017, a Las Vegas physician practicing in pain management was found guilty of conspiracy to distribute controlled substances, distribution of controlled substances, money laundering and structuring of money transactions, after prescribing large amounts of legal opioids for no legitimate medical purpose.

Because criminals are aware of CTR requirements, they have developed methods for introducing their illegal proceeds into the financial system. But what about a doctor who receives credits from insurance companies or deposits cash under the guise of cash co-payments?

Financial institutions should consider being even more sensitive to potential BSA/AML concerns if they operate in a geographic region that has been affected by opioids. As proven by some of the recent examples, even traditionally legal transactions can be involved in threat finance.

HOW TO BEST PROTECT YOUR INSTITUTION:
THREE MODELS FOR TRANSACTION MONITORING SYSTEM GOVERNANCE

The Importance of Transaction Monitoring Systems

In order to effectively and correctly detect and report suspicious activity, financial institutions must ensure their transaction monitoring systems are working as intended. Sensing red flags in the way funds flow through different streams in the financial landscape is the easiest way to detect illegal operations.

Transaction monitoring systems help to accurately highlight unusual or potential suspicious activity and help management document and explain filtering criteria and thresholds, as well as how both are appropriate for the bank's risk appetite (per regulatory guidance expectations).

Transaction Monitoring System Review and Governance

Because transaction monitoring systems are so critical to an institution's AML program, institutions must review and tune these systems to make sure they:

1. Validate all the required inputs (e.g., reconciliations)
2. Establish alert triggers (e.g., rules, parameters, thresholds, etc.) that relate back to specific identified risks

There are three testing level options Capco considers best practice in this area, depending on an institution's specific factors. There is overlap between the different testing models, but each level is unique in its comprehensiveness, and stands alone as a full testing process.

Based on an institution's risk appetite and regulatory requirements, it can decide to test its systems at any level — the first level being the most basic review and the last being a true model validation. Capco has found that some institutions struggle to differentiate between a systems check (the first two levels) and a true validation (the last level), so we have outlined the three levels.

LEVEL ONE — BSA/AML RULES REVIEW AND TUNING

The first level, a BSA/AML Rules Review and Tuning, is an analysis of the BSA/AML system settings, focused on rules with parameters and thresholds to determine effectiveness in detecting potentially suspicious activity. The main focal points of this type of review are:

- The configuration of the rules used to quantify customer risks and monitor for suspicious activity must be configured to the risks that you are trying to mitigate.
- The effectiveness of a BSA system can be compromised if the system is generating too few or too many alerts.
- Rule tuning is necessary to determine the level of suspicious activity or potentially suspicious activity detected using above and below the line testing.
- A review should focus on understanding where your BSA/AML risk is concentrated based on the AML Risk Assessment.

Questions to Guide the Process

- ☐ When reviewing and evaluating the existing rules and associated thresholds, what certain criteria and parameters will you need to use as filters?
- ☐ How can you ensure effective and optimized application to eliminate redundancies and increase synergies between the different rules?
- ☐ If the system is used for OFAC, how often do you review threshold levels and test for system sensitivity?
- ☐ How and what do you document to guarantee the ability to explain the rationale behind existing rules and associated thresholds, filtering criteria and parameters in relation to your organization's risks?
- ☐ What alignment can you draw between existing rules and potential or confirmed suspicious activity?
- ☐ Do you raise or lower thresholds to test selected rules through above the line and below the line testing?
- ☐ How do you evaluate the adequacy of the existing rules?
- ☐ How often do you implement new, enhanced rules based off the results of internal and external testing?
- ☐ Do existing and new rules ensure effective and efficient monitoring based on your organization's BSA/AML risk profile, including transactions, products and services and geographies?
- ☐ When implementing new rules and associated thresholds do you document and explain the rationale behind the adoption, explaining why they are reflective of your organization's BSA/AML risks?
- ☐ Once new rules have gone into effect, how soon after and with what degree of consistency do you review and evaluate reports on the rules' effectiveness?

engagement opportunity

Capco offers consulting engagements at all three levels of AML system governance review. To learn more about how we can help your institution, please contact allan.cuttle@capco.com.

LEVEL TWO — BSA RULES VALIDATION

The second level, BSA Rules Validation, focuses on data integrity controls; risk scoring analysis and testing; and suspicious activity analysis and rules. This leverages the reconciliation work already done and performs sample testing to ensure its adequacy; and it validates the rules, providing a reasonable assurance that the rules are functioning as designed and assisting the institution in meeting regulatory requirements.

Questions to Guide the Process

The second level of testing builds on the first level. It therefore includes most aspects of the first level, and the guiding questions for a BSA/AML Rules Review and Tuning should also guide a BSA Rules Validation. In addition to the guiding questions listed above, in the second level, your institution should evaluate:

- ☐ How do you review data flow documentation to ensure a complete understanding of the source and sufficiency of transaction data imported from the core banking systems and manual sources into the BSA/AML application?
- ☐ Does your review validate data integrity and quality of data reconciliation tests that confirm that the BSA/AML solution is accurately and completely capturing relevant customer, transactions and other data elements?
- ☐ How often do you run reconciliation tests? What is the retesting structure?
- ☐ Are the system reconciliations in place sufficiently documenting data accuracy and completeness between the core banking systems and the BSA/AML monitoring system?
- ☐ What is the clearing process for unprocessed items in the system?
- ☐ When testing alerts generated from the BSA/AML solution is the sample pool sufficient to verify that alerts are generated based on the rules set within the solution?
- ☐ Do the reports the BSA/AML solution generates identify gaps in the system?

LEVEL THREE – BSA SYSTEM MODEL VALIDATION

The third level, BSA System Model Validation, is the most comprehensive and complex so you can be confident that your BSA/AML systems are performing as intended. A BSA System Model Validation puts the BSA/AML solution into a test environment for analysis, developing and running comprehensive scenario tests from the core banking applications through the BSA/AML solution to ensure your institution obtains the desired alert results.

The critical elements covered in a true Model Validation are:

- Is the BSA/AML application configured properly to deal with the BSA/AML risks inherent within your organization's environment?
- Is the data mapping complete?
- Is the BSA/AML application properly capturing all data being fed by the core systems and/or any other types of transactional systems within your organization's environment? Is the aggregation of transaction and account data occurring within the BSA/AML application (this covers both the number count of transactional items and the classification of the data between the core and the BSA/AML filter)?
- Is the system operating as intended, free of system defects?
- Are the BSA/AML rules and/or parameters set within the system generating the appropriate alerts?
- Is the BSA/AML system generating all the appropriate business and regulatory reports?

A best practice for System Model Validations is to perform them during the initial system set-up/ configuration or 6 – 12 months after the system is up and running, and again annually or earlier, if there are substantial system changes or if new core systems have been installed, impacting the data flowing to the BSA/AML monitoring system.

The Process

Capco recommends working with an independent third party for a full model validation, as the outside analysis and recommendations could prove beneficial to an otherwise insular validation system. The steps in this process could include:

- Preparing a test strategy to clearly document the detailed test scope, approach for test planning, test execution and defect management process suitable to the test environment and test data available at your organization
- Detailing the input and output for model testing and test closure process
- Performing data migration testing to validate the flow of data from core systems to the BSA/AML system and analyze all types of transactional data
- Preparing test scenarios and test scripts for each BSA/AML rule or parameter, using both simulated and historical data, customer risk ratings, all utilized modules of the BSA/AML application and all system-produced reports
- Performing specific types of retesting
- Reviewing and analyzing findings

Some Questions to Consider

- ☐ What is your organization's system used for (e.g., customer risk scoring, suspicious activity identification, CTR filings, 314a filings, and/or OFAC)?
- ☐ If used for suspicious activity, has the system been previously validated? If so, when? Are there any examiner comments in this area?
- ☐ Have the rule settings ever been reviewed?
- ☐ Are system parameters reviewed? If so, how often?
- ☐ Is there a process for reconciling data?
- ☐ Does your organization maintain a current data map for the interface between the core system and any other system and BSA system?
- ☐ What features should the validation cover (e.g., customer risk scoring, suspicious activity rules, CTR filings, 314a searches, and/or OFAC)?

OTHER BEST PRACTICES

In addition to performing proper systems testing, some best practices for institutions hoping to enhance their AML efforts include:

- Ensure your institution follows a formal change management process.
- Establish clear roles and separation of duties within your AML regime.
- Provide access to configuration settings only to those who need access, and limit systems access for others.
- Ensure participants at all levels not only understand their roles and access settings, but also know who to reach out to with questions.
- Define the IT power and long-term costs necessary to run your system and ensure the system will operate within these parameters.

CONCLUSION

With AML risks constantly shifting and developing, it is critical for institutions to ensure high-level safeguarding. Vigilant system governance is critical to supporting a robust and effective AML system, and defining a validation or review process is the only way to ensure your systems are capable of genuine monitoring against the most sophisticated money launders and financial threat. ❖

WILL REGULATORS 'LIKE' YOUR INSTITUTION'S SOCIAL MEDIA MARKETING?

While advertising products and services on social networking websites can be beneficial for financial institutions, there are some risks involved. Recent developments call into question the legality of certain aspects of this type of marketing.

On August 17, 2018, the U.S. Department of Housing and Urban Development (HUD) announced a formal complaint against a popular social media website for violating the Fair Housing Act. HUD asserts that landlords and home sellers can engage in housing discrimination using the website's advertising platform when utilizing "targeted advertising" tools.

HUD's complaint outlines that advertisers can control which users receive housing-related ads based upon the user's race, color, religion, sex, familial status, national origin, disability and/or zip code. The basis of HUD's formal complaint is that the site then invites advertisers to unlawfully discriminate, targeting certain audiences and excluding others, which HUD believes limits housing options for certain protected classes.

The Fair Housing Act prohibits specific types of discrimination in housing transactions, including print and online advertisement, based on protected classes identified in applicable laws:

- Title VI of the Civil Rights Act of 1964 (race, color, national origin)
- Section 109 of the Housing and Community Development Act of 1974 (race, color, national origin, religion, sex)
- Section 504 of the Rehabilitation Act of 1973 (disability)
- Title II of the Americans with Disabilities Act of 1990 (disability)
- Architectural Barriers Act of 1968 (disability)
- Age Discrimination Act of 1975 (age)
- Title IX of the Education Amendments Act of 1972 (sex)

HUD began investigating the website's advertising platform after an article in 2016 claimed the social media-based company provided advertisers opportunities to exclude specific ethnic groups from receiving ads. The investigation halted earlier this year, but HUD Secretary Ben Carson reopened the investigation after fair housing groups filed lawsuits against the company in March 2018, claiming ad placement still discriminated against women, veterans with disabilities and single mothers.

HUD's complaint alleges the website's platform violates the Fair Housing Act by enabling advertisers to, among other things:

- Display housing ads either only to men or women
- Not show ads to users interested in an "assistance dog," "mobility scooter," "accessibility" or "deaf culture"
- Not show ads to users categorized as interested in "child care" or "parenting," or show ads only to users with children above a specified ag
- Display/not display ads to users categorized as interested in a particular place of worship, religion or tenet, such as the "Christian Church," "Sikhism," "Hinduism" or the "Bible"
- Not show ads to users categorized as interested in "Latin America," "Canada," "Southeast Asia," "China," "Honduras" or "Somalia"
- Draw a red line around zip codes and then not display ads to users who live in specific zip codes

The U.S. Attorney for the Southern District of New York also filed a statement of interest, which HUD joined, in U.S. District Court on behalf of a number of private parties fighting the website's advertising practices.

This formal complaint comes at a time when questions are emerging within the financial services industry regarding online advertising, and particularly advertising through social media websites.

Using character-limiting social media platforms to advertise banking products, including mortgage loans

Currently, some platforms limit characters allowed in a post, with one of the leading platforms of this type limiting posts to 280 characters, and not fully supporting the use of graphics. Accordingly, incorporating the mandatory "Equal Housing Lender" logo for consumer residential real estate-secured lending advertisements is not feasible and the medium does not support this type of advertisement. However, there may be other platforms that allow proper inclusion of necessary logos and language.

Multiple regulatory agencies have put out guidance to help financial institutions stay in compliance when using social media or for online advertising.

- **The Financial Industry Regulatory Authority (FINRA)** was the first to publish guidance in this area. The most pertinent FINRA publications are Regulatory Notice 10-06 (Guidance on Blogs and Social Networking Web Sites); Communications Rule 2210-2216 (Communications With the Public); and Regulatory Notice 17-18 (Guidance on Social Networking Websites and Business Communications).
- **The Securities and Exchange Commission (SEC)** published related items, such as the Division of Investment Management's Guidance on the Testimonial Rule and Social Media.
- **The Federal Financial Institutions Examination Council (FFIEC)** released guidance in 2013.
- **The Office of Compliance Inspections and Examinations (OCIE)** published a Risk Alert in September 2017 titled, "The Most Frequent Advertising Rule Compliance Issues Identified in OCIE Examinations of Investment Advisers," which discussed areas of concern within social media utilization for marketing purposes.

Staying up-to-date with these guidances, notices and alerts is critical, as the industry has seen repercussions for those with violations in social media marketing practices. On July 10, 2018, the SEC charged five separate parties for using social media and the internet in ways that violated the Testimonial Rule under the Investment Advisers Act of 1940, and there have been other instances of regulatory scrutiny for advertising on social networking sites that may limit an institution's ability to remain compliant with applicable laws and regulations.

Considerations in Social Media Marketing

Required statements: Make sure your institution follows the guidelines noted above for required statements, such as FDIC membership for FDIC-insured products or the official advertising statement of NCUA membership.

Privacy and data security guidelines: Consider which areas of the Gramm-Leach-Bliley Act or other privacy regulations may extend to how you will protect clients that interact with certain types of advertisements through social media platforms. Be sure there are specific programs in place to take down any information about users under age 13 that are posted publicly in reaction to any marketing efforts (e.g., within a comment on a post).

Unsolicited messaging: Carefully assess how your organization is using certain features of social media marketing, including direct messaging within certain platforms and garnering email addresses through user interaction via social media sites.

Disclosures: Advertisers should place disclosures as close to the triggering claim as possible, and only use hyperlinks for disclosures in certain situations (in most cases, not for product cost, health or safety issues) and language used for hyperlinks should alert the user to the hyperlink's criticality or significance.

Endorsements and testimonials: It is important to be aware of guidelines for the use of endorsements and testimonials in advertisements online, especially through blogs or social media influencers. This includes monitoring the truthfulness of and ability to substantiate any claims and the requirements, if any, to disclose certain connections. Many firms choose to block or not utilize testimonials altogether to avoid the legal complexities of endorsements, as is the case with investment advisers who are prohibited from using testimonials.

Formatting: It is best practice to ensure any marketing pushed through social media platforms are formatted for the specific website or app on which an advertisement may appear, to guarantee that all precautions taken for compliance with disclosure size and proximity requirements remain intact when viewed on various devices.

Vendor management: Institutions that use third parties for marketing efforts (creative, copy, design, etc.) and corresponding media buys must be careful to cautiously govern each outside party. Just as with other marketing materials and social media placements, an institution needs to review through a compliance lens each advertisement that a third party creates or places. The targeting and placement criteria should be crystal clear.

With a vast number of consumers active on social networking sites, and the comparatively low costs associated with advertising on these platforms, many institutions hope to utilize popular sites and applications to grow their customer base or promote new products or services. Moving forward with these initiatives requires special attention, and compliance officers should ensure that they are up-to-date with changing developments that will likely impact marketing and communications plans. ❖

ABOUT CAPCO

Capco is a global business and technology consultancy dedicated to the financial services industry, plus a dedicated energy division. Capco delivers innovative solutions in Banking & Payments, Capital Markets and Wealth & Asset Management, designed to withstand market forces, continual regulatory change and increasing consumer demand.

WORLDWIDE OFFICES

Bangalore	Hong Kong	Singapore
Bratislava	Houston	Stockholm
Brussels	Kuala Lumpur	Toronto
Chicago	London	Vienna
Dallas	New York	Warsaw
Dusseldorf	Orlando	Washington, DC
Edinburgh	Paris	Zurich
Frankfurt	Pune	
Geneva	São Paulo	

CONTACT US

Capco Center of Regulatory Intelligence
1101 Pennsylvania Ave., NW Suite 300
Washington, DC 20004
E: capco.cri@capco.com
P: 202.756.2263

@CAPCO

WWW.CAPCO.COM

CAPCO