acxell

ADVISOR

Fall 2024

Review, revise, repeat

IS IT TIME TO REVISIT YOUR ANTI-MONEY LAUNDERING PROGRAM?

HOW TO MANAGE LIQUIDITY RISK FROM CRYPTO-ASSETS

BEST PRACTICES FOR BUILDING CUSTOMER LOYALTY

BANK WIRE

acxell

www.acxellrms.com 877.651.1700

Review, revise, repeat

IS IT TIME TO REVISIT YOUR ANTI-MONEY LAUNDERING PROGRAM?

If you haven't reviewed your bank's anti-money laundering program recently, it may be time for an update. Here's a look at the latest developments.

NEW TERMINOLOGY AND RULES

One sure sign that your program is outdated is if you still call it a Bank Secrecy Act/Anti-Money Laundering (BSA/AML) program. These days, most banking regulators are using the term Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT). The new terminology reflects changes made by the Anti-Money Laundering (AML) Act of 2020 and aligns more closely with the AML/CFT national priorities outlined by the Financial Crimes Enforcement Network (FinCEN) in 2021. To ensure that your program passes muster with examiners, review these priorities and make any necessary changes to comply with the new law.

One of the most significant provisions of the AML Act was to establish a federal beneficial ownership registry administered by FinCEN. By allowing law enforcement and financial institutions (with permission from their customers) to view the information in the registry, the act makes it harder for criminals to hide behind shell companies to conceal their identities. The law also expands and enhances criminal penalties for BSA violations, increases rewards and protections for whistleblowers, and strengthens the U.S. government's subpoena power over foreign bank accounts.

In addition, bankers should familiarize themselves with FinCEN's recently proposed rules, which would impose new AML/CFT requirements on financial institutions. (See "Proposed rules would beef up AML/CFT requirements" on page 3.)

UPDATED PRIORITIES

Among FinCEN's AML/CFT priorities are:

Corruption. According to FinCEN, combating corruption is a "core national security interest." Banks play a key role in this effort, because "corrupt actors and their financial facilitators may seek to take advantage of vulnerabilities in the U.S. financial system to launder their assets and obscure the proceeds of crime." Banks should consult FinCEN advisories regarding corruption-enabled human rights abuses to identify typologies and red flags associated with these abuses.

Cybercrime. Specific concerns are:

- Cyber-enabled financial crime,
- Ransomware attacks, and
- The misuse of virtual currencies that "exploits and undermines their innovative potential, including through laundering of illicit proceeds."

PROPOSED RULES WOULD BEEF UP AML/CFT REQUIREMENTS

On June 28, 2024, FinCEN announced a proposed rule designed to strengthen and modernize financial institutions' Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) programs. Among other things, the proposed rule, if adopted, will require banks to implement the following proactive measures:

- Maintain effective, risk-based and reasonably designed AML/CFT programs. (By explicitly requiring programs to be *effective*, the proposed rule would impose new burdens on banks.)
- Review FinCEN's AML/CFT priorities and incorporate them, as appropriate, into their risk-based programs.
- Conduct formal risk assessments to evaluate their exposure to AML/CFT risks.
- Ensure that their AML/CFT programs are administered by people in the United States and are overseen and approved by their boards of directors.

Also, on July 19, 2024, the federal banking agencies jointly announced a proposed rule that would update their AML/CFT program requirements and align them with FinCEN's proposed rule. Notably, the agencies' proposal would require that banks' AML/CFT officers be "qualified" and that independent testing of banks' AML/CFT programs be conducted by qualified personnel or outside parties.

FinCEN notes that financial institutions "are uniquely positioned to observe the suspicious activity that results from cybercrime," and encourages them to share this information with one another under the BSA's safe harbor provisions.

Foreign and domestic terrorist financing. Because terrorist groups need financing to operate, FinCEN reminds banks of their obligation to identify potential terrorist financing transactions and file suspicious activity reports (SARs). It also notes that banks must comply with required sanctions programs and be aware of terrorists or terrorist organizations on government-issued sanctions lists.

Fraud. According to FinCEN, fraud is believed to generate the largest share of illicit proceeds in the United States. Fraudulent proceeds may be laundered by "money mules" and transfers through offshore and cybercriminals' accounts.

Transnational criminal organization (TCO) activity. According to FinCEN, drug trafficking organizations and other TCOs are increasingly turning to "professional money laundering networks that receive a fee or commission for their laundering services." These groups specialize in laundering proceeds generated by others.

Drug trafficking organization (DTO) activity. FinCEN notes that both the proceeds of illicit drugs (which may be laundered in or through the United States) and the drugs themselves contribute to a "significant public health emergency." DTOs tend to rely on professional money laundering networks in Asia (primarily China) that facilitate exchanges of Chinese and U.S. currency or serve as brokers in trade-based money laundering schemes.

Human trafficking and human smuggling. Financial activity related to human trafficking and human smuggling can "intersect with the formal financial system at any point during the trafficking or smuggling process." Networks use a variety of methods to move illicit proceeds, including cash smuggling and front companies.

Proliferation financing. Proliferation support networks seek to exploit the U.S. financial system to move funds used to acquire weapons or support state-sponsored weapons programs. FinCEN notes that global correspondent banking is a principal vulnerability and driver of proliferation financing risk in the United States.

REVIEW AND UPDATE

Banks should evaluate their AML/CFT programs and revise them, as needed, to incorporate FinCEN's priorities and reflect any changes in their risk profiles. Staying on top of the latest rules regarding money laundering is essential for any community bank going forward. ■

HOW TO MANAGE LIQUIDITY RISK FROM CRYPTO-ASSETS

Last year, there were several notable bank failures, some of which were connected to market vulnerabilities associated with cryptocurrency and crypto-asset-related (CAR) entities. In the wake of these failures, the federal banking agencies provided banks with guidance on managing crypto-asset risks.

First, the agencies issued a *Joint Statement on Crypto-Asset Risks to Banking Organizations*, which warned banks in general about crypto-asset risks. Later, the agencies focused on liquidity with their *Joint Statement on Liquidity Risks to Banking Organizations Resulting from Crypto-Asset Market Vulnerabilities*.

HIGHLIGHTS OF THE GENERAL GUIDANCE

The first statement warns banks of several key risks associated with crypto-assets and participants in this sector. They include:

- Fraud and scams among crypto-asset sector participants,
- Legal uncertainties related to crypto-asset custody practices, redemptions and ownership rights,
- Inaccurate or misleading representations and disclosures by CAR companies,
- Volatility in the crypto-asset markets,
- Susceptibility of stablecoins (cryptocurrency whose value is tied to that of another currency, commodity or financial instrument) to run risk,
- Contagion risk stemming from interconnections among sector participants (that is, opaque lending, investing, funding, service and operational arrangements), which may also present concentration risks,
- Lack of maturity and robustness of risk management and governance practices in the crypto-asset sector, and
- Heightened risk associated with open, public or decentralized networks (that is, lack of oversight, absence of contracts or standards, vulnerabilities to cyber-attacks, outages, lost or trapped assets, and illicit finance).

According to the statement, the agencies "believe that issuing or holding as principal crypto-assets that are issued, stored, or transferred on an open, public, and/or decentralized network" is likely to be inconsistent with safe banking practices. They also have serious concerns about safety and soundness issues raised by business models that are concentrated in CAR activities or have concentrated exposures to the crypto-asset sector.

HIGHLIGHTS OF THE LIQUIDITY GUIDANCE

The statement on liquidity risks notes that certain funding sources from CAR entities present heightened liquidity risks, including:

Deposits by CAR entities for their customers' benefit. The stability of these deposits may be driven by the behavior of these customers or market dynamics, not just the CAR entity itself.

Deposits that constitute stablecoin-related reserves. These deposits, the statement explains, are "susceptible to large and rapid outflows stemming from, for example, unanticipated stablecoin redemptions or dislocations in crypto-asset markets."

To address these risks, the statement encourages affected banks to implement certain liquidity risk management practices, including actively monitoring liquidity risks inherent in CAR funding sources and maintaining effective risk management controls. In addition, these banks should make sure to understand the direct and indirect drivers of crypto-asset deposit behavior and the susceptibility of such deposits to unpredictable volatility.

It's also important for banks to assess the liquidity risks associated with potential concentrations or interconnectedness of deposits from CAR entities. And they'll need to incorporate liquidity risks and funding volatility associated with CAR deposits into their contingency funding plans (that is, via liquidity stress testing and other risk management processes). Finally, performing robust due diligence and ongoing monitoring of CAR entities that open deposit accounts (including scrutinizing the representations they make to their customers) is key.

FOLLOW THE RULES

Finally, the statements remind banks to comply with all applicable laws and regulations. For insured depository institutions, this includes, but isn't limited to, compliance with the FDIC's "Brokered Deposit Rule" and, as applicable, the "Consolidated Reports of Condition and Income (Call Report)" filing requirements. Crypto-assets are now a fact of life, and community banks must take care to manage them properly. ■

BEST PRACTICES FOR BUILDING CUSTOMER LOYALTY

In today's rapidly shifting marketplace, community banks must ensure they're proactive in anticipating — and responding to — customer needs. This will help retain customers and maintain bank profitability over time. Here are some best practices to help banks compete and thrive.

STUDY CORE DEPOSITS

A good first step is to identify your core deposits and develop an understanding of customer behaviors. Differentiate loyal, long-term customers from those motivated primarily by interest rates. A core deposit study can help you distinguish between the two types

of depositors and predict the impact of fluctuating interest rates on customer retention. Banking regulators strongly encourage banks to conduct these studies as part of their overall asset-liability management efforts.

Core deposit studies assess how much of your bank's deposit base is interest-rate-sensitive by examining past depositor behavior. They also look at factors that tend to predict depositor longevity. For example, customers may be less likely to switch banks if they have higher average deposit balances and use multiple banking products (such as checking and savings accounts, mortgages and auto loans).

UNDERSTAND YOUR CUSTOMERS

To build customer loyalty, it's critical to actively engage your customers. According to research by Gallup, engaged customers are more loyal, and they're more likely to recommend the bank to family and friends. They also represent a bigger "share of wallet" (that is, the percentage of a customer's banking business captured by the bank).

Recent retail banking studies show that fewer than half of customers at community banks and small regional banks (less than $40 billion in deposits) are actively engaged. The percentages are even smaller at large regional banks (over $90 billion in deposits) and nationwide banks (over $500 billion in deposits). That's the good news. The bad news is that 50% of customers at online-only banks are fully engaged.

So, how can community banks do a better job of engaging their customers to compete with online banks? The answer lies in leveraging their "local touch" by knowing their customers, delivering superior service, and providing customized solutions and advice. To do that, banks must ensure that their front-line employees — tellers, loan officers, branch managers and call center representatives — are fully engaged in their jobs.

Encouraging employees to engage with customers has little to do with competitive salaries and benefits. Rather, it means providing employees with opportunities for challenging work, responsibility, recognition and personal growth.

IMPROVE AND STREAMLINE ONLINE BANKING

An increasing number of customers — younger people in particular — use multiple channels and devices to interact with their banks. These include online banking, mobile banking applications and two-way texting.

To build loyalty, banks should enable customers to use their preferred channels and ensure that their experiences across channels are seamless. And don't overlook the importance of social media platforms. Younger customers are more likely to use these platforms to recommend your bank to their friends and families.

STAY IN TOUCH WITH CUSTOMERS

In addition to these best practices, ensure excellent customer service by regularly touching base with bank customers, through online surveys, phone calls or in-person conversations. This will help reveal what bank services are meeting their needs, and what services might be improved, leading to a better outcome for all concerned. ■

BANK WIRE

SHOULD YOUR BOARD APPROVE LOANS?

Bank Director's "2023 Governance Best Practices Survey" found that a majority of banks approve individual loans at the board level, though the practice appears to be declining. According to the survey, 64% of respondents said that their board (or a board-level committee) approves individual loans, and 36% said the board approves loan policies or limits. Four years earlier, Bank Director's "2019 Risk Survey" reported that 77% of respondents said their board approved individual loans.

But *should* directors be approving individual loans? There's no one right answer to this question. Some bankers believe that additional oversight by experienced directors provides significant benefits, especially for larger loans. On the other hand, board involvement in individual loan approvals may raise potential directors' liability concerns. Plus, taking loan approvals off directors' plates can free them up to focus on strategic planning, risk management and other "big picture" activities. ■

SEC'S NEW CLIMATE DISCLOSURE RULES

The Securities and Exchange Commission's controversial climate disclosure rule has been placed on hold as a result of harsh criticism and multiple legal challenges. The SEC adopted the rule earlier this year in an effort to enhance and standardize climate-related disclosures by public companies and in public offerings. Among other things, the rule requires companies to disclose material climate-related risks, efforts to mitigate those risks, board oversight of climate-related risks, and costs associated with severe weather events and other natural conditions. Although the rule mainly affects large companies, smaller companies could experience a trickle-down effect if, for example, large companies ask their vendors, suppliers or other business partners to collect and share climate-related information.

If the rule survives legal scrutiny, it will have a significant impact on many companies' financial statements. However, as of this writing, the rule's future is highly uncertain. ■

THIRD-PARTY RISK MANAGEMENT: AN INSTRUCTION MANUAL

In 2023, the federal banking agencies published *Interagency Guidance on Third-Party Relationships: Risk Management*. It outlines sound risk-management principles for banks when contemplating relationships with fintech companies and other providers.

In May 2024, the agencies published *Third Party Risk Management: A Guide for Community Banks*. Although the guide isn't a substitute for the interagency guidance, it provides community banks with valuable tips for managing third-party relationships. The 30-page guide offers potential considerations and examples in connection with risk management, the third-party relationship life cycle, and governance related to third-party risk. It also includes an appendix that lists various government resources community banks can use in their third-party risk management efforts. To find the guide, go to Occ.com and click on news releases for 2024. ■

acxell ("acxell") has been meeting the specific risk management needs of community banks of all sizes since 1991. As a high quality and affordable alternative to other firms, acxell provides internal audit, regulatory compliance, BSA/AML, information technology, SOX/FDICIA and enterprise risk management review services and software. acxell is exclusively dedicated to the banking industry, providing clients with dedicated, focused and hand-held services reflective of a wide range of skills, experience and industry expertise. As a Firm, we have also been proactive in assisting our clients with the designing, implementation and testing of the internal control environment to assist management with the attestation requirement under the Sarbanes-Oxley Act.

acxell's uniqueness is characterized by its experienced staff and partners. Their hands-on involvement on each engagement provides our clients with a wide range of skills, experience and industry expertise. We employ the use of Subject Matter Experts — designated individuals performing audits in their specific field of expertise. The use of such professionals provides a unique value-added approach that is both efficient and productive.

We believe that a significant aspect of our services is our degree of involvement and responsibility to assist management by making suggestions for improvement, keeping them informed of professional developments and by acting as an independent counsel and sounding board on general business matters and new ideas.

We pride ourselves in our ability to provide effective and practical solutions that are commensurate with our clients' needs by emphasizing high-quality personalized service and attention. Our services are truly customized.

For **Solutions** *to your risk management needs, please contact our service coordinators at (877) 651-1700, or log-on to www.acxellrms.com to learn more.*

www.acxellrms.com

Headquarters:
646 US Highway 18
East Brunswick, NJ 08816

Offices:
New York, NY
Philadelphia, PA
Chicago, IL
Miami, FL