acxell

ADVISOR

Winter 2022

FinCEN's NATIONAL AML/CFT PRIORITIES SET THE TONE

KEEPING BRANCH BANKING PROFITABLE IN THE DIGITAL AGE

Protect your data
WHAT'S YOUR BANK'S PLAN TO COUNTER RANSOMWARE ATTACKS?

BANK WIRE

acxell

www.acxellrms.com 877.651.1700

FinCEN's NATIONAL AML/CFT PRIORITIES SET THE TONE

In June 2021, the Financial Crimes Enforcement Network (FinCEN) issued its first set of government-wide priorities (the Priorities) for anti-money laundering and countering the financing of terrorism (AML/CFT). As required by the Anti-Money Laundering Act of 2020 (AML Act), the Priorities identify and describe the most significant AML/CFT threats currently facing the United States.

FinCEN will soon issue regulations that instruct banks and other financial institutions on how to incorporate the Priorities into their risk-based AML/CFT programs. In addition, though not required by the AML Act, federal banking agencies plan to revise their Bank Secrecy Act (BSA) regulations to explain how the Priorities will be incorporated into banks' BSA requirements.

WHAT ARE THE PRIORITIES?

FinCEN developed the Priorities after consulting with various Treasury Department offices, federal and state regulators, law enforcement, and national security agencies. Pursuant to the AML Act, FinCEN will update the Priorities at least once every four years in consultation with the same government agencies. These updates will reflect new and emerging threats.

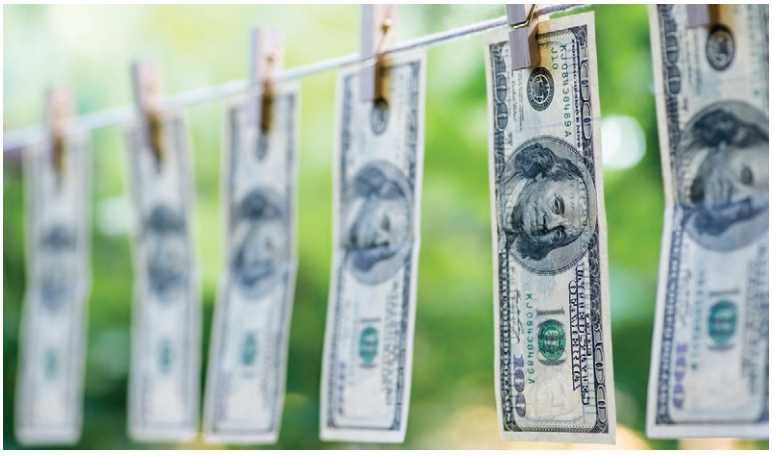
The Priorities are:

Corruption. According to FinCEN, corrupt actors often exploit vulnerabilities in the U.S. financial system to launder assets and obscure crime proceeds. Past advisories on human rights abuses enabled by corrupt foreign political figures describe typologies and red flags that can help banks identify these actors and activities.

Cybercrime. Treasury is particularly concerned about cyber-enabled financial crime, ransomware attacks and misuse of virtual assets to launder illicit proceeds. Referencing past FinCEN and Treasury advisories regarding ransomware and COVID-19-related cybercrime, the Priorities note that banks are uniquely positioned to observe suspicious activity related to cyber-enabled financial crime and other cybercrime.

Terrorist financing. International and domestic terrorists require financing to support members, fund logistics and conduct operations. So, preventing such financing is essential to U.S. counterterrorism efforts. The Priorities remind banks of existing obligations to file suspicious activity reports (SARs) on potential terrorist financing transactions, follow requirements for reporting violations that require immediate attention and comply with required sanctions programs.

Fraud. The Priorities emphasize that fraud — including bank, consumer, health care, securities and tax scams — is believed to generate the largest share of illicit proceeds in the United States. These proceeds may be laundered through a variety of methods, including transfers through accounts of offshore legal entities, accounts controlled by cyberactors and



money mules. Of particular concern are business email compromise and, most recently, COVID-19-related schemes.

Transnational criminal organization activity. These organizations — which may be involved in cybercrime; drug, wildlife, human, and weapons smuggling or trafficking; intellectual property theft; and corruption — are priority threats due to the "crime-terror nexus" of their illicit activities. According to the Priorities, these organizations are increasingly relying on professional money laundering networks.

Drug trafficking organization activity. Drug trafficking organizations tend to rely on Asian professional money laundering networks that facilitate exchanges of Chinese and U.S. currency or serve as money brokers in trade-based money laundering schemes. The Priorities note a substantial increase in complex schemes involving Mexican drug trafficking organizations that launder narcotics sale proceeds through Chinese citizens residing in the United States, including the use of front companies or couriers that deposit these proceeds in the banking system.

Human trafficking and smuggling. Human trafficking and smuggling networks use various mechanisms to move illicit proceeds, including cash smuggling by individual victims and sophisticated operations involving professional money laundering networks and criminal organizations. They may establish shell companies to hide the true nature of their business. They also may receive payments through such methods as funnel accounts and trade-based money laundering schemes.

Weapons proliferation financing. The principal threat here comes from proliferation support networks. These networks include individuals and entities, such as trade brokers and front companies, that exploit the U.S. financial system to move funds used to acquire nuclear, chemical or biological weapons or to further state-sponsored weapons programs. The principal driver of proliferation financing risk in the United States is global correspondent banking, due to its central role in processing U.S. dollar transactions.

WHAT THE PRIORITIES MEAN FOR COMMUNITY BANKS

The Priorities issued by the Financial Crimes Enforcement Network (FinCEN) will have a major effect on large, globally active financial institutions. (See main article.) But all community banks face some degree of anti-money laundering and countering the financing of terrorism (AML/CFT) risk. Increasingly, criminals are seeking out smaller banks in an effort to avoid the more rigorous AML/CFT programs at larger banks.

To assess risk, community banks should ask the following questions about their products and services, customers and geographic footprint:

- Do you have a significant volume of electronic payments, such as wire and ACH transfers?
- Do your customers make use of electronic banking services, such as remote deposit capture or online account opening?
- Are a significant number of customers cash-intensive businesses, such as liquor or convenience stores?
- Does your customer base include foreign entities or individuals?
- Do you do significant business with nonbank financial institutions, such as casinos or money service businesses?

WHAT'S NEXT?

Banks aren't required to take any action with respect to the Priorities until final regulations are issued. When that happens, banks will need to review and incorporate, if appropriate, these Priorities based on their broader risk-based AML/CFT programs. Although it's not certain when regulations will be finalized, it's a good idea for banks to begin evaluating the potential risks associated with the products and services they offer, the customers they serve and the geographic areas in which they operate. ■

KEEPING BRANCH BANKING PROFITABLE IN THE DIGITAL AGE

The COVID-19 pandemic has led to an increase in online banking. However, the transition to virtual banking was already well underway. As community banks look to the future, they need to re-imagine branch banking for the digital age. This means strengthening what's working and getting rid of what isn't. Direct banking at branches can still be vital to community banks' financial health as long as they measure branch performance and correct as necessary.

CUSTOMER LOCATION

A significant challenge in measuring branch performance is assigning customers to particular locations. Traditional measures (such as new accounts opened or teller activity) no longer suffice. Just because a customer opened an account at a branch doesn't necessarily mean that account should count toward the branch's performance.

What if the customer relocated? What if he or she uses more than one branch? What if the customer does everything online and doesn't visit branches at all? There are no easy answers to these questions. To get an accurate picture of branch performance, banks need to develop models that better reflect a branch's interactions with customers and its contribution to the bank's overall performance.

MEASUREMENT STRATEGIES

Some banks are developing point systems to measure the value of products sold, customer service and retention. For example, core accounts like checking accounts generally are more valuable than CDs, which often constitute "hot money" — that is, funds frequently transferred between financial institutions in an attempt to maximize returns. The analysis might be different, however, if a checking account has a small average monthly balance or if a CD has a relatively long term.

For services, one set of point values might be assigned to transaction processing — such as cashing checks or accepting deposits — with higher values assigned to loans or consultative services.

According to financial services technology provider Fiserv, customers with one banking product stay with a bank around 18 months on average. The average relationship increases to four years for customers with two products and to almost seven years for customers with three products. So, branches with more customers purchasing multiple products tend to contribute more value. And transfers of funds among branches affect branch profitability.

DIFFERENCES IN MARKETS

Too often, banks' business development plans fail to reflect the differences among their branches' local markets, which can be dramatic. Many simply allocate their budgets uniformly among locations and

demand that each branch achieve similar profitability and growth goals.

There are two problems with this approach. First, it establishes unachievable goals for branches in some markets, while allowing other locations to coast. Second, it may cause a bank to miss opportunities to enhance branch performance.

A better approach is to benchmark the bank's performance against that of its peers. After identifying areas in which performance is falling short, the bank can examine individual branches, analyze their local markets and develop strategies for enhancing performance.

It's important to analyze each branch's current customer base as well as the various commercial and consumer segments that make up its local market. Armed with this information, you can develop marketing strategies that make the most of each location's unique profitability and growth opportunities.

For example, a branch in an area with a lot of high-income consumers might target those consumers and also focus on cross-selling to existing customers. (Of course, it's important to keep in mind fair lending exposure and Community Reinvestment Act considerations.) As noted above, providing multiple products to customers improves retention rates. On the commercial side, analyzing local markets may reveal opportunities to serve previously untapped commercial sectors or business niches.

ANALYSIS AND MEASUREMENT ARE KEY

Your community bank will thrive if its branches thrive. Understanding your local customers and their banking preferences has never been more challenging — or more important. Closing branches if they're no longer profitable is one solution. But developing them in ways that make them more useful to customers might be the best strategy over the long run. ■

Protect your data

WHAT'S YOUR BANK'S PLAN TO COUNTER RANSOMWARE ATTACKS?

Cybersecurity continues to be a key risk that businesses face today, and banking is among the industries most affected by cyberattacks. Some experts estimate that around a quarter of all malware attacks target financial institutions. Of particular concern are ransomware attacks, which have increased dramatically in the past couple of years.

The threat of ransomware is so serious that the National Institute of Standards and Technology (NIST) — developer of a widely used cybersecurity framework — recently published a draft Cybersecurity Framework Profile for Ransomware Risk Management (the Ransomware Profile).

RANSOMWARE AND RISK MANAGEMENT

Ransomware is a type of malware that encrypts an organization's data. Once malware has infected a system, the attackers demand payment in exchange for the encryption key that unlocks the data. In some cases, they may also steal an organization's information and

demand additional payment to avoid disclosure of that information to authorities, competitors or the public.

The Ransomware Profile outlines several basic preventive steps organizations can take to protect themselves against the ransomware threat, including:

- Use antivirus software at all times,
- Keep computers updated with the latest security patches,
- Segment internal networks to prevent malware from proliferating among potential target systems,
- Continuously monitor for indicators of compromise or active attack,
- Block access to potentially malicious web resources,
- Allow only authorized apps, and avoid use of personal apps — such as email, chat and social media — on work computers,
- Use standard user accounts, rather than accounts with administrative privileges, whenever possible,
- Restrict personally owned devices on work networks,
- Educate employees about social engineering (for example, to not open files or click on links from unknown sources without scanning for viruses or taking other precautions), and
- Assign and manage credential authorization for all enterprise assets and software, and periodically verify that each account has only the appropriate access.

Organizations also should take steps that will help them recover from future ransomware events, including developing and implementing rigorous backup and incident recovery plans.

BACKUP STRATEGIES AND INCIDENT RESPONSE PLANS

Simply keeping backups of data isn't enough. Any significant gaps in recoverable data or delays in restoring systems can be devastating for banks. So, they must back up data daily and test and periodically validate it. Also, banks should store backups offline to prevent a ransomware attack.

> ANY SIGNIFICANT GAPS IN RECOVERABLE DATA OR DELAYS IN RESTORING SYSTEMS CAN BE DEVASTATING FOR BANKS.

A well-designed backup strategy is worthless, however, without a solid incident response plan. This critical step helps banks restore systems quickly and minimize downtime in the event of a ransomware or other attack. A cyberattack is highly stressful. So, to avoid a paralyzing panic, your response plan should provide step-by-step instructions on who does what and when. The plan also should be kept offline to ensure that it's accessible if your systems aren't.

BE PREPARED

All banks should have a comprehensive cybersecurity plan to prevent ransomware and other cyberattacks and to minimize damages should an attack occur. If your bank doesn't have a plan or you're unsure whether your plan provides the protection you need, talk to your advisors about conducting a cybersecurity risk assessment. ■

BANK WIRE

GET READY FOR GENERAL QUALIFIED MORTGAGE FINAL RULE

In April 2021, the Consumer Financial Protection Bureau (CFPB) delayed the deadline for compliance with its revised general qualified mortgage (QM) rule to October 1, 2022. But it's a good idea for banks to start reviewing the requirements now and determine how they'll need to update their procedures to incorporate the new rule. QMs — which avoid certain risky features and meet other requirements designed to make them safer and easier for borrowers to understand — are presumed to comply with ability-to-repay rules.

Currently, for a loan to be a QM, the borrower must have a total monthly debt-to-income ratio (including mortgage payments) of 43% or less. The revised rule greatly simplifies the definition of a QM by discarding the debt-to-income limit in favor of a price-based model. For loan applications received on or after March 1, 2021, but before October 1, 2022, lenders have the option of complying with either the current or the revised general QM loan definition. (Note: Separate rules apply to "seasoned" QMs.) ■

NEW LEASE ACCOUNTING RULES BACK ON BANKS' RADAR

After several delays — including a one-year postponement due to COVID-19 — the new lease accounting standard is scheduled to take effect for private companies for fiscal years beginning after December 15, 2021, and interim periods within fiscal years beginning after December 15, 2022. If your compliance efforts have been on hold, it's time to ramp them up again. The upcoming transition to the new rules may influence current negotiations between banks and their loan customers, and banks that lease their facilities, equipment or other fixed assets should prepare for the rules' potential impact on their balance sheets and regulatory capital. Plus, the standard's transition approach may require banks to implement certain changes before the rules take effect. ■

GUIDE TO CONDUCTING DUE DILIGENCE ON FinTECH COMPANIES

Community banks are under increasing pressure to provide their customers with digital products and services, and many banks are partnering with financial technology (FinTech) companies as a strategy for developing innovative, customized, cost-effective solutions. These partnerships can be complex ventures that involve a variety of risks, so thorough due diligence is critical. To assist banks with these efforts, federal banking agencies have published "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks."

The due diligence practices described in the guide are voluntary and don't establish any new risk-management requirements. But they provide valuable guidance on what community banks should be looking for when they evaluate potential FinTech providers in six areas: 1) business experience and qualifications, 2) financial condition, 3) legal and regulatory compliance, 4) risk management and controls, 5) information security, and 6) operational resilience. ■

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