protiviti®
Face the Future with Confidence

Compliance Insights

Your monthly compliance news roundup

May
2020

BSA/AML Examination Manual Updates from FFIEC

On April 15, 2020, the Federal Financial Institutions Examination Council (FFIEC) released updates to the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) examination manual. The manual is used to evaluate an institution's compliance with the Bank Secrecy Act and anti-money laundering requirements. This is the first and a much-anticipated revision since 2014. Although the updates do not establish any new requirements, they offer valuable insight and transparency into the examination process and highlight the importance of a risk-based evaluation.

The updates to the manual are focused on the following examination activities: scoping and planning, the BSA/AML risk assessment, evaluating the BSA/AML compliance program and developing conclusions and finalizing the exam. The scoping and planning section outlines areas of focus and emphasizes the need to perform evaluations tailored to an institution's risk profile for money laundering, terrorist financing, and other financial crimes. Consideration of the risk profile allows the exam to focus testing and assessment on the areas identified as the greatest risk to the institution, new risks, or a change in risk profile.

The manual further provides procedures and guidance for assessing the adequacy of an institution's BSA/AML compliance program. This includes the institution's risk assessment, internal controls, independent testing, the BSA compliance officer role and responsibilities, and training. The guidance indicates that the adequacy of the BSA/AML compliance program should be assessed based on the institution's client types, the volume of transactions, business with high-risk jurisdictions, and additional risk factors that are specific to the bank and defined in the BSA/AML risk assessment. In addition to defining the risk assessment factors, the manual suggests that an institution's risk assessment "quantify" those risks (e.g., adding in data to support transaction volumes) to improve the institution's own understanding and assessment of those risks.

Overall, there is a shift in the updated manual from assessing the effectiveness of the institution's BSA/AML compliance program to evaluating its adequacy. The updated manual states that conclusions should relate to the adequacy of the institution's BSA/AML compliance program, explaining that "minor weaknesses, deficiencies, and technical violations alone are not indicative of an inadequate BSA/AML compliance program."

Next steps for institutions include ensuring that their risk assessments are up to date, that they include specific risk categories (e.g., products, services, customers, and geographic locations) and supporting metrics, and that they are specifically customized to the institution's money laundering risks. These steps will allow each institution to identify its highest-risk areas and focus risk mitigation efforts and will serve to inform examiner scoping of future exams.

Joint Advisory on North Korea Cyber Threat

On April 15, 2020, the U.S. State Department, the Department of Homeland Security, the Treasury Department and the Federal Bureau of Investigation (FBI) issued a joint advisory relating to North Korea's malicious cyber activity: "Guidance on the North Korean Cyber Threat." In the advisory, the United States claims North Korea has been employing an array of cyberattacks to steal and launder money, extort companies and use digital currencies to generate revenue for its weapons of mass destruction (WMD) and ballistic missile programs.

The advisory was published after the Financial Action Task Force (FATF) issued its February 2020 call-to-action notice, which urges North Korea to address deficiencies in its anti-money laundering/countering the financing of terrorist (AML/CFT) regime, and acknowledges serious threats posed by the nation's illicit activities to the international financial system. The advisory provides guidance to financial institutions on designing and implementing AML/CFT and sanctions compliance controls to more effectively mitigate threats posed by North Korea's cyber activities.

It also highlights the activities which target the financial sector and pose the greatest threat to the integrity of the international financial system. Specifically, the advisory states that cyber-enabled financial theft, extortion campaigns, and cryptojacking (a scheme intended to compromise a victim's computer and steal its computing resources to mine digital currency), are all examples of common but sophisticated tactics used by North Korea to raise revenue to fund its WMD ambitions. Additionally, the advisory details cyber incidents that the U.S. government has publicly attributed to North Korea-sponsored cyber actors, including the 2016 Bangladesh Bank heist, when cyber criminals allegedly stole $81 million from Bangladesh's central bank.

The advisory outlines measures to counter cyber threats posed by North Korea, including raising awareness of cyber threats, sharing technical information, implementing and promoting cybersecurity best practices, notifying law enforcement, and strengthening AML/CTF controls.

The advisory serves as a reminder of FATF's 2019 guidance requiring its jurisdictions to regulate and supervise digital asset service providers and mitigate against risks when engaging in digital currency transactions. Financial institutions are reminded of their obligations to develop and maintain effective AML/CTF programs. They should ensure that their compliance programs include robust internal controls relating to financial crimes and cybersecurity, and take targeted action to assess their exposure to North Korea's financial crimes to protect themselves against potential financial loss, reputation risk, government enforcement action, and national security.

CFPB Issues Office of Servicemember Affairs' 2019 Annual Report – Highlights

The 2019 Annual Report from the Office of Servicemember Affairs (OSA), which covers the period of October 1, 2018 to September 30, 2019, highlights the OSA's Servicemembers Civil Relief Act (SCRA) activities in fiscal year 2019 (FY19). OSA, which is part of the Consumer Financial Protection Bureau (CFPB), issues the annual report to increase the financial well-being of military families and address the financial concerns that military consumers face. In the latest report, servicemembers from all 50 states and the District of Columbia submitted a total of 34,600 complaints, with most complaints originating from California, Texas and Florida.

The top five complaint categories were: credit reporting, debt collection, mortgages, credit cards, and checking/savings accounts. Many complaints pertained to incorrect credit reporting followed by problems with inquiries into existing credit or consumer credit reporting issues. Others relate to attempts to collect debt not owed for miscellaneous products and services such as phone bills, health club memberships, and home utility services, followed by credit card debt. The majority of mortgage complaints center on challenges faced during the payment process. Complaints regarding credit cards cover a variety of risk areas, including problems with purchases shown on statements, concerns with fees, interest or other credit card features, as well as issues with getting a credit card and making payments. Most complaints around checking or savings accounts related to issues with managing the account.

The remaining smaller category of complaints deal with student loans, vehicle loans or leases, money transfers, money services and virtual currencies, personal loans, prepaid

cards, payday loans, credit repair, and title loans. Additionally, most of the complaints about personal and payday loans involve military consumers indicating that they were charged unexpected fees or interest.

Protecting Our Servicemembers' Financial Well-Being

As the public health crisis posed by COVID-19 worsens, many Americans across the country are experiencing significant financial shock. Servicemembers, veterans, and military families are no exception. Although veterans and active duty servicemembers continue to receive their benefits and pay, some military personnel and their families are facing financial strain due to lost employment or changes in military orders.

The sacrifices made by the men and women who answer the call to serve their country is well deserving of our gratitude and appreciation. Financial institutions play a big role in not only honoring but in protecting those who protect us. Considering the issues raised in the OSA report and the financial turmoil the pandemic has created, financial institutions should carefully consider or scrutinize the following strategies and practices to help military families address their financial challenges:

- Provide free credit monitoring for active duty military members.
- Provide financial counseling resources for military families experiencing COVID-19-related financial hardships, such as the Military OneSource site that offers free financial counseling services.
- Direct military families to service relief organization such as the Army Emergency Relief, the Navy-Marine Corps Relief Society, the Coast Guard Mutual Assistance, and the Air Force Aid Society if they need emergency help.
- Develop or enhance financial literacy programs designed for military members. For example, USAA is helping our veterans transition back to civilian life by providing a calculator they can use to understand the difference in taxes, helping them gauge what kind of salary they need to maintain their quality of life.
- Adopt new and innovative technologies, from AI-driven, self-guided financial advice to comprehensive digital money management tools, to help military members stay in the know about their finances at all times.

Our nation's active duty and reserve servicemembers, veterans, and their families face different challenges due to their unique living circumstances. Many live and work under

trying conditions (such as deployments and uncertain return dates from deployments), and when it comes to transitioning back into civilian life, servicemembers face new and unique challenges. By easing (via financial education programs, enhanced monitoring programs) military consumers' burden of financial hardship, financial institutions can strengthen their business relationships with military consumers while helping them to better navigate their finances during their military careers and beyond.

About Protiviti

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Through its network of more than 85 offices in over 25 countries, Protiviti and its independent and locally owned Member Firms provide clients with consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit.

Named to the 2020 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 60% of Fortune 1000® and 35% of Fortune Global 500® companies. The firm also works with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

protiviti®