

Top Five FinCrime Challenges Expected in 2021

TERRI LUTTRELL, CAMS-AUDIT



INTRODUCTION

Living through a global pandemic was unimaginable until it happened. The year has been tough for everyone, both personally and economically, but we are beginning to see the light. Whatever lies ahead for the financial crimes (FinCrime) industry in 2021, we will be better equipped after the events of 2020. Despite the challenges financial institutions and the FinCrime industries have endured in 2020, the hope is that these industries will react and adapt in a way that will make them even stronger moving into the new year.

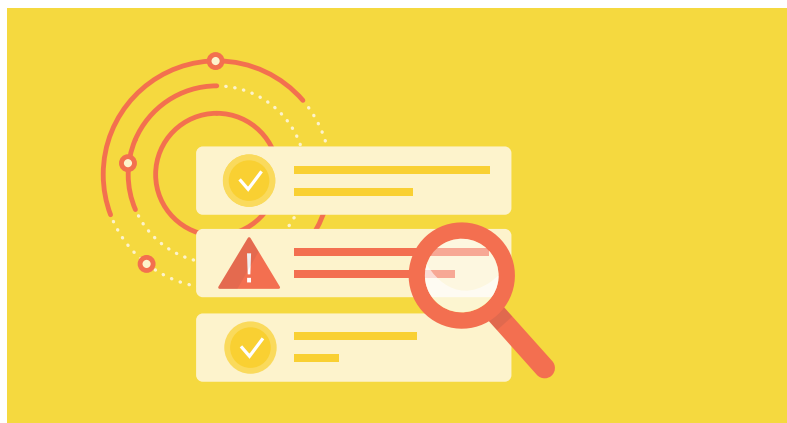
During a recent series of Abrigo FinCrime roundtables, industry experts from both small and large banks and credit unions discussed what they believe to be the biggest challenges within FinCrime in 2021.

1. THE COVID-19 IMPACT

The pandemic has had – and continues to have – a significant impact on financial institutions. It is no surprise that this tops the list of hot topics for FinCrime professionals going into 2021. Although there are vaccines on the horizon, the industry clearly understands that they will be dealing with COVID-19-related issues for the first part of 2021, at the very least. According to the [FBI and the Secret Service](#), COVID-19-related fraud is at a crisis level, and the agencies expect that this upward trend will continue for some time. As with any national disaster, fraud, scams, and thefts have proven to be a continuing challenge for financial institutions. This trend, combined with federal economic relief packages like the \$2 trillion Coronavirus Aid, Relief, and Economic Security (CARES) Act, has created the perfect storm.

The magnitude of the pandemic and the accompanying bad actors is unprecedented. The additional fraud alerts have overwhelmed anti-money laundering (AML) and fraud departments as they struggle with the increase in alerts and the accompanying suspicious activity reports (SARs). Both AML and fraud investigators are detecting COVID-19 related fraud, and the importance of collaboration between the teams is especially important. A financial institution would not want to find themselves in a position of filing two separate SARs on the same activity.

While it is understood that AML and fraud investigations overlap at times, COVID-19-related fraud has increased the necessity for teams to collaborate and cross-train. Many financial institutions have moved to combine these teams or are seriously considering this. The challenge with combining current AML and fraud staff is that the investigative skill set of each group is very different. While AML investigators look for patterns, the source and use of funds, and historical transaction data, fraud investigators work real-time, to prevent potential hard dollar losses. If using cross-team resources for investigations, it is important to cross-train the investigators on any lacking analytical skills. After the pandemic, your FinCrime team will be even stronger.



Any discussion of COVID-19-related fraud for 2021 would not be complete without a mention of Paycheck Protection Program (PPP) fraud. The program distributed more than \$521 billion in loans. While applications ended August 8, PPP fraud is still being detected and will continue into 2021. All financial institutions, regardless of size, are vulnerable to this threat, as we've seen by the recent [Department of Justice indictments](#). Law enforcement estimates that between 10-12% of the total PPP loans are fraudulent. As FinCrime investigators review their portfolios and follow the use of funds, it is important for them to partner with law enforcement and report detected PPP fraud as soon as possible. If a financial institution is not reviewing their PPP portfolio they may want to consider doing so, as regulators are expecting it.

Another COVID-19-related challenge faced by financial institutions is the shift to remote working. Most community banks and credit unions were not poised for the sudden change, lacking the technology to efficiently communicate and operate remotely. For FinCrime staff, where collaboration is crucial, the lack of internet bandwidth, laptops, and communication tools made their day-to-day analysis more difficult. Moving into 2021, many institutions are establishing a hybrid approach, positioning many non-customer facing staff to work remotely. The industry is beginning to embrace this new norm, upgrading their technology and implementing new ways to effectively communicate online. However, it's important that community banks and credit unions recognize that continuously advancing their technological footprint should be an ongoing priority – not a one-time investment.

2. CDD/EDD REGULATORY EXPECTATIONS

The continued importance of customer due diligence (CDD) and know your customer (KYC) cannot be understated. These expectations are not just critical during the onboarding process, but throughout the relationship with the customer. CDD is widely considered the fifth pillar of Bank Secrecy Act (BSA) compliance in the FinCrime industry, with significant regulatory scrutiny. In fact, most consent orders issued in 2020 included a section of CDD deficiencies.

How should a financial institution ensure that they will not be one with a criticized CDD program? Start at the beginning of current CDD processes: data. If incorrect or missing data is flowing into your suspicious activity monitoring program, the CDD program will be inherently deficient. A periodic data integrity review with further verification by an external audit source is critical to ensure all relevant activity is being monitored.



Financial institutions should focus on training front line staff to understand the importance of capturing required CDD information. No one in the institution will know these customers better than the front line, like tellers and lenders. Obtaining the customer information upfront will prevent most questions from the FinCrime team down the line. CDD is more than a checkbox, and it's important that every single person in the institutions understands that they each play a critical role in safeguarding the institution and our overall national security. Some financial institutions have had success with front line accountability processes, such as compliance scorecards that are part of their compensation program. This can only be successful if there is support from senior management, which sets the tone from the top.

Ongoing monitoring, or enhanced due diligence (EDD), is an equally important aspect of a strong CDD program. More guidance has been issued in 2020, including changes to the BSA Examination Manual, which stresses that CDD and other BSA program components should be risk-focused. There is not a one-size-fits-all rule for how a financial institution should conduct their EDD. For example, a risk assessment should be conducted on all higher-risk customer categories, segmenting certain persons/industries based on their unique risk. Just because a customer is a private ATM owner, for example, does not mean that he or she must be considered high-risk solely on that attribute. The risk assessment should be thorough enough to support any risk rating program developed for the institution.

Analyzing actual customer transaction activity against expected activity obtained from the customer is a regulatory requirement. Some institutions are creating a more risk-focused approach to the questions asked at account opening, which enables the institution to ask fewer, but more reliably answered questions to address greater risk. This strategy strengthens customer satisfaction at onboarding without sacrificing knowing your customer. It is crucial to ensure that this process, if reduced, is substantiated by your risk assessment.

EDD reviews are required periodically on all customers with heightened risk. These reviews should also be risk-based, including the frequency of reviews. Rather than using a moderate-risk category, many institutions have started using two or more high-risk categories to indicate higher risk.

Many regulatory consent orders criticize the lack of thoroughness of the EDD reviews performed by an institution. Periodic reviews should be thorough, analyzing the entire customer relationship over a predetermined period of time, based on risk. A review narrative should be as inclusive as a SAR narrative, including information as to why the customer is or is not transacting suspicious activity.

3. POSSIBLE CHANGES TO BSA REGULATIONS

On October 23, 2020, the Federal Reserve Board and the Financial Crimes Enforcement Network (FinCEN) jointly issued a [notice of proposed rulemaking](#) (NPR). The proposed amendments, if passed, would modify two rules that have been part of the Bank Secrecy Act (BSA) regulations since 1995.

The NPR would change the reporting requirements of the [recordkeeping rule](#) for collecting and retaining certain funds transfer information, lowering the threshold from \$3,000 to \$250. It would also change the [travel rule](#) for transmitting information on funds transfers cross border from \$3,000 to \$250. While the initial response from many financial institutions is that this lowered amount is unreasonably low, others recognize that some of the most detrimental financial crimes are funded with very small transaction amounts, many of which cross borders. Financial institutions will want to proactively consider the impact on current procedures and processes and be poised to implement if passed in 2021.

An additional component of the NPR would include convertible virtual currency (CVC) and digital assets used for legal tender with the intent to clarify the meaning of “money” as used in these same rules. Virtual currency is here to stay. In fact, some banks have developed their own virtual currency. If an institution lacks extensive knowledge in this area, it will be critical that it gets up to speed in. While there are many legitimate uses of virtual currencies, bad actors globally are using this [payment source](#) for nefarious purposes, including terror financing. The concepts of tokens, blockchain, wallets, and other virtual currency terms can be confusing. Build a foundation with the basics, then learn the intricacies as you go. A strong knowledge in virtual currency will strengthen your FinCrime program as this risk increases.

The FinCEN Files refers to leaked documents from FinCEN involving more than 200,000 suspicious financial transactions totaling over \$2 trillion.

Other regulatory changes, or at the least regulatory expectations, may stem from the release of the [FinCEN Files](#). The FinCEN Files refers to leaked documents from FinCEN involving more than 200,000 suspicious financial transactions totaling over \$2 trillion. The documents reveal how criminals have money laundered “dirty money” throughout some of the world’s largest banks. More than 2,000 SARs were leaked, heightening concerns over filing repeated SARs on customers without closing accounts. Regulations require financial institutions to know their customers, and if they detect suspicious activity, it is their responsibility to stop the movement of illicit funds. If your financial institution has not administered an exit plan for suspicious relationships, it should be top-of-mind in 2021.

4. THE CHANGING POLITICAL CLIMATE

COVID-19 is not the only notable challenge seen throughout 2020. The political climate in the U.S. has reached new boiling points, marked by civil unrest and calls for social justice, a contentious presidential election, and, unfortunately, the threat of violence from domestic extremist groups. The FBI continues to call the current civil unrest and political climate a threat to national security and has successfully thwarted many domestic attempts of violence. The recent arrest of a group who conspired to kidnap the governor of Michigan highlights the escalating threats that domestic terrorist groups pose.

Terrorist financing typologies from abroad have been on the radar of FinCrime investigative teams since the 9/11 attacks. This type of illicit activity is especially difficult to detect due to the typical lower dollar amounts involved, but continuous guidance from the Federal Financial Institutions Examination Council (FFIEC) and the Financial Action Task Force (FATF) has assisted financial institutions by referencing red flags indicative of terrorist financing. Domestic terrorism is a relatively new term that FinCrime teams have not had in their BSA policies and risk assessments until recently, and no FinCEN guidance or red flags have been issued up to this point.

The FBI defines the two types of terrorism as:

International terrorism: Violent, criminal acts committed by individuals and/or groups who are inspired by, or associated with, designated foreign terrorist organizations or nations (state-sponsored).

Domestic terrorism: Violent, criminal acts committed by individuals and/or groups to further ideological goals stemming from domestic influences, such as those of a political, religious, social, racial, or environmental nature.

Federal law defines domestic terrorism in the U.S. legal code, but it is not codified as a law that can be prosecuted. When indicted, these extremists must be charged for crimes other than terrorism, such as hate crimes or weapons possession. While prison sentences can be lengthy, the label "terrorist" cannot be applied under current law. The first amendment protects free speech, including extremist language, and therefore cannot be prosecuted.



Domestic terrorism, regardless of legal status, is a present and serious threat to the U.S. It is critical that FinCrime professionals work with law enforcement to better detect and prevent future domestic terrorist attempts. If international terrorism is difficult to detect with guidance and red flags issued, many institutions wonder how they can successfully monitor for domestic terrorism without such guidance. While it's certainly a challenge, the first step is to identify this threat in the financial institution's risk assessment and create a risk-based approach to mitigate this risk.

In recent remarks at the September 2020 Association of Certified Anti-Money Laundering Specialists (ACAMS) annual conference, Frederick Reynolds, Global Head of Financial Crime Legal at Barclays Bank and a former FinCEN Deputy Director, advised institutions to avoid stereotyping, noting that domestic extremist groups come from all walks of life. Some emerging financial indicators will be useful, such as analyzing basic know your customer policies and examining the flow of funds, particularly into and out of higher-risk charities that could be funneled to extremist causes. Reynolds further proposed a six-stage analytical approach for financial institutions to implement for detecting possible radicalization:

- Look for signs of radicalism with open source search tools
- Notice and changes in life or financial patterns
- Use keyword detection for expenditures of concern (bomb making materials)
- Question attempts to conceal activity
- Note if the volume of activity intensifies
- Be aware of possible final actions before terror attack (i.e., one-way airfare)

In addition to filing a SAR for suspected domestic terrorism, it is paramount that institutions alert law enforcement immediately upon detection. Financial institutions do not have to be certain; rather, they must only have to suspect a threat to take action. If extremist groups continue to cause threats of violence, this may end up being the most significant challenge faced in 2021.

5. CANNABIS BANKING

Cannabis banking has been a FinCrime hot topic for many years, and it is getting even hotter in 2021. A decade ago, there was not a single state that had legalized recreational use of cannabis. Today, 11 states and Washington, D.C. have now legalized recreational use. In the 2020 election, five more states voted to approve recreational and/or medical cannabis use. While more states are embracing cannabis, the risks associated with banking cannabis-related businesses (CRBs) are still high. Marijuana remains classified as a schedule 1 narcotic in the [Controlled Substances Act](#). Regardless of any state law, marijuana remains illegal at the federal level.

Today, if a financial institution chooses to provide banking services to a CRB, it must determine [which tier level](#) (I, II, III) it is willing to risk. In some communities, the stigma surrounding marijuana could lead to reputational risk for financial institutions, regardless of legal status.

The legalities and risks associated with cannabis banking are complicated. To understand the nuances, it's important to fully understand the language associated with cannabis, including marijuana, hemp, and CBD, and add that to your cannabis-related business risk assessment.

- Cannabis – plant of origin, an herb family
- Marijuana – Species of cannabis, includes tetrahydrocannabinol (THC), gets user high
- Hemp – Species of cannabis, does not include THC over 0.3%, does not get user high
- CBD – Cannabinoid – generally extracted from hemp (oils and tinctures)

An institution's risk assessment should break these down separately. It is common for institutions to be willing to [provide services](#) to a hemp-related company now that hemp is legal at the federal level (if certain criteria is met). However, if THC levels in hemp crops cross the level of 0.3%, it becomes marijuana and illegal crops could be destroyed.



Then there is CBD (hemp derived). It is sold in almost every pharmacy, gas station, and convenience store and most financial institutions do have customers in this category. Institutions should ensure that their CRB risk assessment includes this component of the industry, and they should double-check whether or not their policy states that it will allow certain services to any CRBs. Much like the guidance around the percentage of acceptable sales from lottery sales, CBD sales can be defined as acceptable risk under a certain percentage of sales (say under 10%). A customer attestation should be obtained to transfer the burden of proof on the customer rather than the financial institution.

Financial institutions should also keep their eyes on changes that may happen at the federal level. The House of Representatives has [approved legislation](#) that would decriminalize marijuana and remove marijuana from the Controlled Substances Act. The Marijuana Opportunity Reinvestment and Expungement Act, or MORE Act, would make banking marijuana related businesses less risky, but it is unlikely to be passed in the Senate. As with any Presidential administration change, the future legal status of marijuana is uncertain but may change. It will undoubtedly continue to be a key topic for FinCrime professionals in the coming year. Stay up to date on state and federal legislation and remain diligent in your CDD efforts to truly know who may be a CRB. If you have questions on the laws in your institution's footprint state(s) or neighboring states, refer to the marijuana legality map [here](#).

CONCLUSION

The new year is sure to present anticipation, as well as challenges, for the FinCrime industry in 2021. The information presented in this paper is based on industry professional opinions, from years of research, discussions with regulators, and hands-on experience. It is important to be forward-thinking so that your institution will be ready for whatever 2021 has to bring. The industry has proven its ability to pivot and succeed in the face of a global pandemic and economic crisis. Other challenges to come will certainly be met head on with ease.

ADDITIONAL RESOURCES

Blog: [Will Cannabis Banking Turn Over a New Leaf After COVID-19?](#)

Webinar: [Banking Marijuana-Related Businesses](#)

Webinar: [Politically Exposed Persons and Your Institution: Identifying, Handling, and Banking](#)

Webinar: [Back to Basics: Strategic Due Diligence on Higher Risk Customers](#)

Whitepaper: [Four Key Strategies for a Successful CDD Program](#)

Whitepaper: [PPP Fraud Detection Checklist: Key Due Diligence Elements to Review to Detect PPP Fraud](#)

ABOUT THE EXPERT



Terri Luttrell, CAMS-Audit

COMPLIANCE AND ENGAGEMENT DIRECTOR

[ABRIGO](#)

Terri Luttrell is a seasoned AML professional and former director and AML/OFAC officer with over 20 years in the banking industry. Luttrell has worked in both medium and large community and commercial banks, ranging from \$2 billion to \$330 billion in asset size. She has successfully worked with institutions in developing BSA/OFAC programs, optimizing various automated solutions and streamlining processes while ensuring all regulatory requirements are met.

As the Compliance and Engagement Director at Abrigo Luttrell provides insights that contribute and support long-term banking strategies based on analysis of market and industry trends, competitor developments, and financial and regulatory technology changes. She is an audit-certified anti-money laundering specialist and a board member of the Central Texas chapter of the Association of Certified Anti-Money Laundering Specialists (ACAMS).

ABOUT ABRIGO



Abrigo is a leading technology provider of compliance, credit risk, lending, and asset/liability management solutions that community financial institutions use to manage risk and drive growth. Our software automates key processes—from anti-money laundering to asset/liability management to fraud detection to lending solutions—empowering our customers by addressing their Enterprise Risk Management needs.

Make Big Things Happen. Get started at [abrigo.com](#).

