Anti-Money Laundering Compliance Must Put Officers On Alert

By **Poppy Alexander and Caleb Hayes-Deats** (January 8, 2024)

Poppy Alexander

Caleb Hayes-Deats

Recent government actions against FTX Trading Ltd. and other crypto companies have put a laser focus on corporate compliance failures, and not just for cryptocurrency companies.

Gurbir Grewal, the U.S. Securities and Exchange Commission's Division of Enforcement director, recently reminded compliance personnel that they "serve as the first lines of defense against misconduct."[1] Compliance officers, Grewal warned, thus need to "take the steps necessary to effect compliance."

Grewal's comments reflect the pressure compliance personnel immediately face when misconduct is alleged. Their title alone implies that they should either explain what happened or accept responsibility.

Grewal is far from the first government official to directly scrutinize senior compliance officers. In 2015, then-Deputy Attorney General Sally Yates issued what became known as the Yates Memo, which instructed prosecutors investigating corporations to focus on individuals and hold them accountable alongside their companies.[2]

Yates' successor, Lisa Monaco, doubled down on this policy, publicly declaring in September 2022 that, when it comes to corporate investigations, "the Department's number one priority is individual accountability."[3]

And under another recent U.S. Department of Justice policy, chief compliance officers must now certify the adequacy of their compliance program as part of a resolution of any DOJ action.[4] These policies have resulted in enforcement actions by the DOJ, the U.S. Department of the Treasury, and other regulators that have specifically targeted compliance officers.

Given the threat of personal liability for institutional failings, what can compliance officers do to best protect themselves and their institutions from potential liability for anti-money laundering issues? We suggest adapting the risk assessment process that should be familiar to compliance personnel.[5]

Virtually every compliance officer has undertaken risk assessments for their financial institutions, but few have done so for themselves. The need for a personal risk assessment is particularly acute given the many novel anti-money laundering issues that compliance officers face today.

Conducting a Personal Risk Assessment

The Bank Secrecy Act requires that financial institutions conduct risk assessments to identify potential gaps in their anti-money laundering programs. At the most basic level, a corporate compliance risk assessment involves three steps.

First, the institution evaluates the inherent risk posed by its business profile. The risks that

institutions face vary with the services they offer and the geographies in which they do business.

For example, institutions that do business in Eastern Europe face increased risk of being used for transactions that seek to evade sanctions against Russia. Second, once an institution has identified the specific risks to which it is exposed, it can assess the design and effectiveness of its existing risk-mitigation controls. Ideally, an institution should have specific controls designed to mitigate each of the risks it identified at step one.

Finally, the comparison of the institution's risks and its existing controls should identify its residual risk, the risk that remains despite the institution's efforts. Some residual risk is inevitable, because no program is perfect.

But identifying residual risk with specificity helps determine where an institution can improve and how it can detect problems before they become unmanageable.

Compliance officers can undertake a similar process to assess their own risk of personal liability. First, they should analyze their financial institution's risk profile and identify situations or events that are especially likely to create a risk of personal liability.

Such situations constitute the individual officer's inherent risk that needs to be controlled. In many instances, an individual compliance officer's inherent risk is closely related to the institution's residual risk.

Second, each officer can identify the resources and actions that can act as controls against the inherent risk of personal exposure. These controls include internal reporting mechanisms, advice from in-house attorneys and colleagues, and documentation of how the institution plans to respond to risks.

Finally, the comparison of inherent risk and existing controls should identify the residual risk facing an individual. Compliance officers who identify their residual risk can communicate proactively with their institutions to reduce that risk and develop a plan for responding if it materializes.

Past enforcement actions identify three scenarios that present an inherent risk of individual liability. Most obviously, any compliance officers who knowingly participate in a legal violation will open themselves up to liability.

Second, compliance personnel can face personal liability when they know of, but fail to correct, ongoing institutional violations. For example, the Financial Crimes Enforcement Network brought an enforcement action against Michael LaFontaine, the former chief operational risk officer at U.S. Bank, for failing to correct problems in the bank's anti-money laundering program that subordinates repeatedly called to his attention.[6]

Third, compliance officers face additional scrutiny when they interact directly with regulators. The Office of the Comptroller of the Currency recently charged Rabobank's former chief compliance officer, Laura Akahoshi, with hiding critical information during an investigation of the bank, although the charges were later dropped.[7]

Compliance officers should bear these scenarios in mind when conducting their personal risk assessments.

Recent Trends and the New Risks They Create

A personal risk assessment should be rigorous and must also account for recent shifts in the anti-money laundering compliance landscape. Such an accounting must ask how a compliance officer's institution has responded to the change, what potential risks remain for the officer to navigate, and what controls the officer has for doing so.

In the last two years, compliance programs have experienced a sea change due to the quickly evolving sanctions landscape after the Russian invasion of Ukraine in February 2022.

Governments in the U.S. and abroad have implemented new sanctions against Russian financial institutions, businesses, and individuals to punish Russia and impair its ability to wage war.

Those sanctions have stranded Russian assets abroad and led to no shortage of schemes designed to either repatriate the assets or evade restrictions on their use.

Cryptocurrencies and related businesses present another quickly changing issue that financial institutions must navigate. On one hand, demand for cryptocurrencies has surged since 2020, as they have become more mainstream. But on the other, recent events have highlighted the risk cryptocurrencies pose not just to investors, but also financial institutions.

Recent enforcement actions have underscored the particular risks for anti-money laundering compliance. For example, FinCEN issued an unprecedented order in January 2023 directing financial institutions to cease transactions with the virtual currency exchange Bitzlato based on concerns that Bitzlato was being used to launder funds for ransomware actors operating in Russia.[8]

Next, the everchanging export control rules adopted in response to perceived threats from China increasingly raise anti-money laundering concerns. Financial institutions that support international trade need to monitor whether transactions are being used to evade export controls.

And the Protecting American Intellectual Property Act enacted in 2023 adopts a sanctions-style regime for individuals and entities that the U.S. designates as having engaged in or benefited from significant theft of trade secrets.

Against this increasingly complex compliance backdrop, there is also the growing importance of different whistleblower programs that allow individuals to report suspicions of corporate misconduct to different federal agencies.

The SEC's tip program[9] is now relatively mature, having paid more than $1 billion in awards since its inception.[10] The Commodities Futures Trading Commission's program is equally established.[11] And since 2021, FinCEN has begun implementing a growing whistleblower program that focuses on violations of the Bank Secrecy Act and various sanctions programs.[12]

Although the FinCEN program is still too new to have yet issued a whistleblower reward, the growth of the SEC and CFTC programs suggests that whistleblowers may cause a significant rise in the number of anti-money laundering investigations in the coming years.

No wonder Grewal framed his remarks to compliance officers through the lens of the

whistleblower program, which he called a "critical part of our enforcement efforts."

Strategies for Controlling Inherent and Residual Risk

In such a shifting environment, compliance officers need strategies to mitigate the risks they face. While the appropriate strategies will vary with the precise risks a compliance officer faces, the law and past enforcement actions identify certain overarching themes.

To violate the Bank Secrecy Act, compliance officers must at a minimum act recklessly, which means that they knew of and disregarded a substantial risk of illegality. The simplest way compliance officers can guard against allegations of individual recklessness is by ensuring that their institutions have policies for dealing with known risks, proposing new policies as necessary.

Of course, compliance officers do not always control what policies their institutions adopt. But they can brief their reporting chains on known risks, propose solutions, and document the decision-making process.

Another way that compliance officers can protect themselves — and effectively advocate for change within their institutions — is by enlisting the support of colleagues.

Just as institutions engage third-party auditors and consultants for second opinions, so can compliance officers engage their colleagues. The more compliance personnel agree that a proposal reasonably responds to a risk, the greater the chance that the institution will adopt it, and the lower the likelihood that regulators will view it as reckless, even with the benefit of hindsight.

Robust discussion of different anti-money laundering policies benefits not only individual compliance officers, but also the institutions they serve. A comprehensive decision-making process that solicits the views of compliance personnel, carefully considers those views, and documents a reasoned basis for the ultimate outcome is powerful evidence that an institution did not knowingly or recklessly violate the law.

Transparent decision making also reduces the likelihood a company will face whistleblower claims. Both the SEC's experience and independent studies show that the vast majority of whistleblowers try to raise concerns internally before contacting the government.[13]

Potential whistleblowers who feel that an institution has seriously considered their concerns may never file an outside complaint, even if the institution ultimately disagrees with those concerns.

Just as financial institutions can never eliminate the risk of money laundering, individual compliance officers may not be able to fully shield themselves from the risk of liability. But compliance officers can identify the specific risks they face as well as the mitigation strategies at their disposal.

Doing so can help them understand the threats they cannot avoid and spot problems long before they receive any inquiry from the government.

Poppy Alexander is a partner at Constantine Cannon LLP.

Caleb Hayes-Deats is a partner at MoloLamken LLP. He previously served as an assistant U.S. attorney in the Southern District of New York.

[1] https://www.sec.gov/news/speech/grewal-remarks-nyc-bar-association-compliance-institute-102423.

[2] https://www.justice.gov/archives/dag/individual-accountability.

[3] https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-remarks-corporate-criminal-enforcement.

[4] https://www.justice.gov/opa/speech/assistant-attorney-general-kenneth-polite-jr-delivers-remarks-nyu-law-s-program-corporate.

[5] https://www.federalregister.gov/documents/2022/06/08/2022-12320/agency-information-collection-activities-information-collection-revision-comment-request-bank.

[6] https://www.fincen.gov/sites/default/files/enforcement_action/2023-04-05/Michael_LaFontaine_Assessment_02.26.20_508.pdf.

[7] https://www.wsj.com/articles/bank-regulator-drops-case-against-ex-rabobank-u-s-compliance-chief-549fa78f.

[8] https://www.fincen.gov/news/news-releases/fincen-identifies-virtual-currency-exchange-bitzlato-primary-money-laundering.

[9] https://www.sec.gov/whistleblower.

[10] https://www.sec.gov/news/press-release/2021-177.

[11] https://www.whistleblower.gov/node/2806.

[12] https://news.bloomberglaw.com/us-law-week/fincens-whistleblower-program-sharpens-focus-on-money-launderers.

[13] https://www.sec.gov/files/owb-2021-annual-report.pdf.