

Recent OCC Actions Focus Attention on Financial Crime Controls for Cryptocurrency Custody Businesses

AUGUST 6, 2020

Two recent actions by the Office of the Comptroller of the Currency (OCC)—one enforcement action and one interpretive note—focus attention on the kinds of anti-money laundering (AML) controls needed for banks to custody cryptoassets while meeting their obligations to fight financial crime. While cryptocurrency does have some unique characteristics that make it higher risk than traditional financial services, established frameworks to manage the financial crime risks attendant with correspondent banking and other intermediated businesses can be applied to the cryptocurrency context to mitigate the extant risk in most circumstances.

I. SAFRA BANK ORDER

On January 30, 2020, the OCC entered into a consent order (Order) with M.Y. Safra Bank, FSB over its failure to implement sufficient AML controls in relation to Safra Bank's cryptocurrency customers.¹ This Order appears to be the first known regulatory enforcement action taken by the OCC against a bank for AML failures related to cryptocurrency customers, and the OCC's Order emphasizes the importance of developing and implementing tailored risk-based controls in the cryptocurrency context.

After an investigation that began in July 2019, the OCC determined that Safra Bank failed to address the risks associated with "high risk customer activity flowing to or from high risk jurisdictions."² The OCC further determined that Safra's Bank Secrecy Act/anti-money laundering (BSA/AML) policies, procedures, and controls were deficient and thus inadequate to identify suspicious transactions. Specifically, the OCC found that Safra Bank violated 12 C.F.R. §§ 21.21 and 163.180 by failing to develop and implement a reasonably designed BSA/AML compliance program, and that it failed to adequately identify suspicious transactions and to file suspicious activity reports (SARs) when required to do so.³

Safra Bank's due diligence and AML program failures were related to the bank's onboarding of "digital asset customers"—cryptocurrency-related money service businesses (MSBs), including "digital currency exchangers, digital currency ATM operators, crypto arbitrage trading accounts, blockchain developers and incubators, and fiat currency MSBs."⁴ The OCC's investigation concluded that Safra Bank accepted these customers "without sufficient consideration of the

BSA/AML risks and failed to implement commensurate controls” to address those risks.⁵ In addition to these failures in customer due diligence, the OCC noted Safra’s failure to monitor and investigate suspicious transactions and timely file SARs.

In other words, at least some of Safra Bank’s cryptocurrency customers were engaged in high-risk transactions that could have generated SAR filing obligations. But because Safra Bank’s controls (including its transaction monitoring program) were insufficient, the bank may have failed to file SARs when required to do so.

Pursuant to the Order, Safra Bank must take a number of steps to remediate the deficiencies in its BSA/AML compliance program. These measures include the appointment by the board of directors of a compliance committee; the augmentation of the BSA officer’s resources and expertise; and adaptations to the written BSA/AML compliance program so the bank appropriately monitors for and reports suspicious activity.

Developing an effective framework to evaluate and mitigate financial integrity risk in the context of cryptocurrency clients takes on particular salience in light of the OCC’s July 2020 interpretive letter confirming that national banks may offer cryptocurrency custody services.⁶ The interpretive letter is part of a broader effort by the OCC, especially under Commissioner Brian Brooks, the former general counsel of the cryptocurrency exchange Coinbase, to ensure that the OCC’s regulations on digital activities by banks “continue to evolve with developments in the industry.”⁷

II. CRYPTOCURRENCY RISKS

Cryptocurrencies are digital representations of value that use cryptography to secure and verify transactions as well as to control the creation of new tokens.⁸ The common understanding that dealing in cryptocurrency tokens poses increased financial integrity risks stems from some of the characteristics of cryptocurrencies that distinguish them from traditional fiat currency. While there are thousands of cryptocurrency tokens in existence, and different currencies have different characteristics, certain core features found across nearly all cryptocurrencies increase their general risk profile.

First, cryptocurrencies may enhance the anonymity of the senders and receivers of value because there often is no centralized counterparty capable of linking digital identifiers to real-world identities.

Second, cryptocurrencies are often disintermediated. That is, participants on a decentralized network can transact in cryptocurrencies in a peer-to-peer fashion via a blockchain (a distributed ledger that maintains a record of balances in the cryptocurrency ecosystem), without the involvement of a regulated financial institution. Counterparties in cryptocurrency ecosystems therefore may be able to transact without having undergone the AML reviews required by regulated financial institutions.

Third, cryptocurrencies enable near-real-time irrevocable settlement. The absence of a central counterparty or coordinating mechanism to conduct book transfers to reverse fraudulent or other problematic transactions further enhances the risks involved in cryptocurrency transactions.

Finally, cryptocurrencies have global reach. Cryptocurrency networks allow individuals to conduct transactions with individuals and entities from around the world.

III. ESTABLISHED FINANCIAL INTEGRITY RISK MANAGEMENT FRAMEWORKS

The unique characteristics of cryptocurrencies therefore present higher risk to financial institutions considering banking cryptocurrency businesses. This risk is enhanced by the fact that cryptocurrency issuers and exchanges also often act as financial intermediaries, conducting transactions on behalf of underlying customers, which may also be the case when banks provide cryptocurrency custody services. In some instances those custody services will be on behalf of a bank's customer only, but in other instances the customer (such as a cryptocurrency investment fund) will be an intermediary, and title to the cryptoassets will rest with the underlying clients of the bank's customer. In these cases there is risk—in particular sanctions risk, but also money laundering risk—inherent in the intermediated nature of the relationship.

Notwithstanding the intermediated nature of the financial integrity risks, the Bank Secrecy Act and its implementing regulations (collectively, the BSA)⁹ covering foreign correspondent accounts, and certain practices among regulated financial institutions with respect to treatment of registered investment advisors (RIAs), reflect established frameworks for mitigating financial integrity risks resulting from certain types of intermediated relationships. The core components of these financial integrity risk management frameworks may be applicable in managing comparable risks in the cryptocurrency context, particularly with respect to cryptocurrency intermediaries like exchanges and cryptoasset investment funds.

Specifically, these risk management frameworks involve understanding the AML and financial integrity controls in place at an intermediary customer, understanding the nature of the services they provide and the geographic areas in which they operate, and understanding the intermediary's customer base at a general level. These risk management frameworks are particularly important for banks offering cryptocurrency custody services, because those custody services will in many cases serve customers of the banks that are acting as intermediaries for those customers' underlying clients, who have an interest in the cryptoassets.

A. Foreign Correspondent Banking

One framework for managing the risks associated with intermediary relationships is the current regulation requiring special due diligence for certain foreign correspondent bank accounts.¹⁰ A foreign correspondent account is an account established at a US bank "for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution."¹¹ Correspondent accounts play a critical role in facilitating cross-border transactions, but they are also susceptible to being exploited for illicit purposes.¹²

Existing US regulations therefore require enhanced due diligence for certain foreign banks. Specifically, covered financial institutions must "[c]onduct enhanced scrutiny of such correspondent account[s] to guard against money laundering and to identify and report any suspicious transactions in accordance with applicable law and regulation."¹³ This enhanced scrutiny requires covered

financial institutions to, for example, obtain and consider information about the foreign bank's AML program and to appropriately monitor transactions to, from or through the correspondent account. Diligence about the foreign correspondent bank's AML program may help US financial institutions understand the general characteristics of the foreign correspondent's products, services and customer base, including, for example, whether the foreign bank does business in countries subject to OFAC embargoes, what its exposure to politically exposed persons is, and whether the foreign correspondent engages in other high-risk activity.

B. Registered Investment Advisors

A second context in which this kind of diligence takes place is the framework through which financial institutions work with registered investment advisors. RIAs are perceived to pose some financial integrity risks because the assets they custody with financial institutions ultimately belong to their underlying customers, not to the RIA, and because RIAs are not currently subject to the BSA. Because those underlying customers generally are not also customers of the financial institution custodialing their assets, that financial institution will not have performed due diligence on the underlying owners of the assets they are custodialing.

Financial institutions often address the risks posed by this intermediated relationship by requiring RIAs to provide representation letters that describe the advisors' own processes for identifying and mitigating the financial integrity risks posed by the clients whose assets financial institutions will custody. In this way, a bank can gain a better understanding of the RIA's clients and thereby manage its own risks by imposing tailored risk-based controls on the RIA.

* * * *

Engaging in similar forms of diligence with respect to cryptocurrency customers can help financial institutions measure and manage the risks attendant with providing them financial services. In this regard, banks should consider asking token issuers, exchanges, investment funds and other digital asset businesses for information about their AML and sanctions compliance programs, their customer bases, their products and services, and their AML program staffing. Additional measures may also be warranted depending on the information banks receive from their cryptocurrency customers. On the basis of this information, financial institutions providing services to digital asset customers should be able to identify the risks attendant with providing them financial services and design an appropriate control framework. While features of certain cryptoassets (e.g., "enhanced anonymity tokens" or "privacy coins") may carry prohibitive BSA risks, in many instances it will be possible to design a reasonable risk-based framework to deal with most digital asset businesses.

The OCC's recent enforcement action against Safra Bank highlights the potential risks involved in onboarding cryptocurrency businesses. While cryptocurrency businesses may present higher risks given the unique characteristics of cryptocurrencies, existing due diligence frameworks demonstrate that those risks can generally be appropriately and adequately addressed. The OCC's recent Order highlights the importance of doing so, and WilmerHale has gained valuable experience in designing such frameworks for clients in the past several years.

-
1. <https://www.occ.gov/static/enforcement-actions/ea2020-005.pdf>.
 2. Order at Art. II, ¶ 1.
 3. *Id.* ¶ 5.
 4. *Id.* ¶ 3.
 5. *Id.*
 6. Office of the Comptroller of the Currency, Interpretive Letter #1170, Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers, July 2020.
 7. Office of the Comptroller of the Currency, Advance Notice of Proposed Rulemaking, National Bank and Federal Savings Association Digital Activities, RIN 1557-AE74, June 4, 2020.
 8. *What is Cryptocurrency. Guide for Beginners*, Cointelegraph.
 9. The BSA implementing regulations are codified at 31 C.F.R. Ch. X.
 10. *See* 31 C.F.R. § 1010.610.
 11. 31 C.F.R. § 1010.605(c)(i).
 12. *See* US Dep't of the Treasury, *National Strategy for Combating Terrorist and Other Illicit Financing* (Feb. 2020).
 13. 31 C.F.R. § 1010.610(b)(1).
-

Authors



**Franca Harris
Gutierrez**

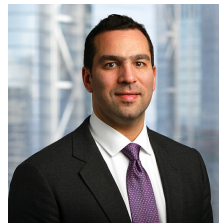
PARTNER

Chair, Financial Institutions
Practice

Co-Chair, Securities and
Financial Regulation Practice

✉ franca.gutierrez@wilmerhale.com

☎ +1 202 663 6557



Zachary Goldman

PARTNER

Co-Chair, Blockchain and
Cryptocurrency Working Group

✉ zachary.goldman@wilmerhale.com

☎ +1 212 295 6309