



“We Don’t Bank Crypto” Isn’t Enough: Banks Need a Strategy for Cryptocurrency

Oct 12, 2020

Categories:

[Blockchain and Digital](#)

[Assets](#)

[Blogs](#)

Authors:

[Courtney Rogers Perrin](#)

[Nancy Eff Presnell](#)

At a recent industry conference, Financial Crimes Enforcement Network (FinCEN) director Kenneth Blanco [made it clear](#) that FinCEN continues to focus on virtual currency. FinCEN is focusing on how to mitigate risks associated with emerging payment systems, including those that utilize cryptocurrency. Blanco emphasized that “these risks are not unique to money services businesses or virtual currency exchangers; banks must be thinking about their crypto exposure as well. These are areas your examiners, and FinCEN, will ask you about when assessing the effectiveness of your AML program.”

What is your bank’s exposure to cryptocurrency?

- Are cold wallets stored in your safe deposit boxes?
- Do you have loans issued where cryptocurrency is the collateral?
- Do you have institutional customers whose dollars are derived from crypto-centric businesses, such as exchanges, money services businesses, or bitcoin ATMs?
- Do you have peer-to-peer virtual currency customers?
- Do you provide wealth management services to customers with crypto assets?
- Do you have emerging payment system clients?

Many banks have taken a “we don’t have clients who are in cryptocurrency, therefore we do not need to draft policies to address cryptocurrency” approach. However, with the sheer size of the virtual currency market, banks may likely have clients with substantial assets in virtual currency or who transact in virtual currency and the denial approach may no longer be sufficient.

Systems to identify customers active in virtual currency, and then to monitor their activities, should, if not already, become part of the bank’s routine. As Director Blanco noted, “What baseline controls do

we have in place to identify customers?" And, "Do we have the tools we need to identify and report potentially suspicious activity occurring through our financial institution?" All of these questions go back to the policies and procedures in place to mitigate risk." When examiners review your Bank Secrecy Program, your bank should provide: a policy that discusses a risk tolerance for virtual currency activity, a risk assessment that discusses such activity, answers to questions regarding virtual currency and customer due diligence, and a mitigation strategy.

For more information, please contact [Courtney Rogers Perrin](#), [Nancy Eff Presnell](#), [John Wagster](#) or any attorney in Frost Brown Todd's [Blockchain & Digital Currency](#) industry team.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.