Armada Business Case

Protecting Banks from FinCEN's Virtual Currency-Related Enforcement Actions

US Banks Prepare for Inevitable Crypto Compliance Examinations in 2021

In 2021, FinCEN, OCC, CFTC, and the SEC are all ramping up cryptocurrency compliance enforcement efforts, requiring financial institutions provide tracking, analysis, and financial crime investigation capabilities for virtual currency-related transactions.

" If banks are not thinking about these issues, it will be apparent when examiners visit. "

-FinCEN Director Blanco, September 29, 2020

US banks are exposed to significant risks from virtual currency because financial crimes, money laundering, cyber security attacks and fraud are, increasingly, funded by or otherwise involve the use of cryptocurrencies. Over $1.3 trillion was transacted in cryptocurrency last year, and this will double year-on-year. Over $1 billion of this was criminal and laundered through banks.

Address Virtual Currency Payment Risks

Virtual currencies are pervasive and have spread to all payment networks. The inability to accurately risk assess these crypto-related payments pose serious reputation and compliance risks, such as:

- Sanctions violations
- Ransomware payments to North Korea and Iran
- BSA money laundering violations
- Hosting unlicensed money transmitters
- Transacting with Crypto Exposed Persons

150+ money mules *transferred* **$108M** in crypto-assets offshore

70% of dark markets *sell* compromised financial products

"We see criminal activity seeking to undermine critical parts of the AML/CFT framework... We also see illicit actors using virtual currency to launder proceeds and buy and sell cyber tools and services on Darknet marketplaces. "

-FinCEN Director Blanco, December 10, 2020

CIPHERTRACE

CipherTrace works with financial institutions and regulators to identify and manage these growing risks.

Comply with Clarified FinCEN Rules for Virtual Currency

FinCEN has classified certain virtual currency companies—including exchanges, bitcoin ATMs and trading desks—as Money Service Businesses, which are required to comply with the BSA. While compliance in the virtual currency industry is rapidly improving, even in the US, CipherTrace KYC research has revealed 55% of crypto MSBs have demonstrably weak KYC processes. Banks have an obligation to verify and perform Enhance Due Diligence (EDD) on MSB customers. This includes unregistered P2P customers that could be using your bank's products.

Detect Cryptocurrency MSBs in Your Bank

In a recent survey, only 22% of FIs claimed to be able to confidently identify cryptocurrency on their payment networks. CipherTrace research shows that 80% of top US retail banks have cryptocurrency Money Service Businesses (MSBs) using their retail and business accounts to perform fiat-to-cryptocurrency transactions.

$25M in crypto laundered *through* **2 Banks + 1 VASP** by **Unlicensed MSB**

Satisfy Suspicious Activity Reporting Obligations

CipherTrace enables your financial institution to detect cryptocurrency-related activity on your credit cards, wire transfers and ACH transactions, and gives you the intelligence needed to file Suspicious Activity Reports related to these transactions.

Identify All Virtual Currency Transactions

CipherTrace enables banks to comply with FinCEN regulations to detect MSBs and other digital asset customers using retail and corporate accounts. This allows your bank to detect cryptocurrency MSBs who are surreptitiously using your bank to operate their money service businesses. Financial Institutions are obligated by FinCEN to detect these operations, perform EDD and treat these operators as MSBs. In some cases, it may be required to report these as potential correspondent banking relationships.

CipherTrace also enables banks to detect virtual currency-related payments, perform VASP due dilligence, and report requisite suspicious activity.

Investigate Financial Crimes

Cybercrimes, including extortion, ransomware and payment fraud, typically have a virtual currency component. CipherTrace blockchain analytics offers financial investigators unprecedented ability to follow the money. CipherTrace provides banks with actionable threat intelligence for cyber security operations. CipherTrace provides names, beneficial ownership, ransomware, dark market, CSAM, and sanctioned entity information as it relates to cryptocurrency transactions involving your customers.

CipherTrace provides telemetry on bank account and IP addresses related to cryptocurrency businesses and malign actors. This informs threat intelligence teams and provides important pivot points in fraud and financial crimes investigations.

Integrate Rapidly with Bank Infrastructure

CipherTrace provides banks with a powerful suite of tools based on the same industry-leading cryptocurrency intelligence and risk data used by DHS, SEC, and the IRS Criminal Division. Off-the-shelf integration with leading AML software, including NICE Actimize, Caseware Alessa, Featurespace, and BAE Systems, simplifies integration and shortens deployment time. CipherTrace Sentry Know-Your-Transaction (KYT) APIs easily integrate with existing systems. Powerful visualization tools help follow the money and perform enhanced due diligence on crypto customers and counter-parties.

About CipherTrace

CipherTrace develops cryptocurrency anti-money laundering (AML)/counter-terrorist financing (CTF), blockchain forensics, crypto threat intel and regulatory solutions. Leading exchanges, banks, auditors, regulators and digital asset businesses use CipherTrace to comply with regulatory requirements, investigate financial crimes, and foster trust in the crypto economy. Founded in 2015 by experienced Silicon Valley entrepreneurs with deep expertise in cybersecurity, eCrime, payments, banking, encryption, and virtual currencies, CipherTrace is backed by top venture capital investors and by the US Department of Homeland Security.
For more information, visit www.ciphertrace.com.