FRAUD RISK IN A CRYPTOCURRENCY WORLD

Businesses and consumers across the globe are quickly adopting cryptocurrencies in daily transactions. And many organizations are scrambling to catch up with this evolving technological innovation. Here's an update on this new means of exchange, key fraud risks and how CFEs can help with the responsible adoption of crypto.

"Innovations in technology often change the world for the better. And yet, criminals, terrorists, and rogue states can use those same innovations for their own illegitimate ends, imposing great costs on the public. Today, few technologies are more potentially transformative and disruptive — and more potentially susceptible to abuse — than cryptocurrency." – U.S. Deptartment of Justice's "Cryptocurrency Enforcement Framework."

With over $2 trillion in circulation, digital assets (aka cryptocurrencies, or "crypto") are increasingly becoming a mainstream form of payment worth more than all physical U.S. dollars and coins currently in circulation. (See "What Happens to the Stock and Cryptocurrencies When the Fed Stops Raining Money?" by Greg Ip, The Wall Street Journal, May 8, 2021, tinyurl.com/kfrkavs5, and "Cryptocurrency is now worth more than all U.S. currency in circulation," by Tony Tran, The Byte, May 9, 2021, tinyurl.com/4w6s7c8u.)

What was first viewed nearly a decade ago as a rogue payment model for criminal activity and ransomware payments is quickly being adopted by many organizations in a variety of industries. Emerging market countries from Pakistan to Vietnam to Nigeria are also seeing an increased use of this form of exchange, while El Salvador last year became the first country to adopt bitcoin as legal tender. (See "Paying with Bitcoin: These are the major companies that accept crypto as payment," by David Walsh, euronews.next, Aug. 30, 2021, tinyurl.com/4un8rwb4; "This map shows where cryptocurrency is taking off around the world," by MacKenzie Sigalos, CNBC, Aug. 18. 2021, tinyurl.com/ysbwub8e; and "El Salvador Has Adopted Bitcoin As Legal Tender — The First Country To Do So," by Tim Padgett, NPR, Sept. 7, 2021, tinyurl.com/27ssewzn.)

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
ALVAREZ & MARSAL'S DISPUTES AND INVESTIGATIONS PRACTICE

This has spurred both regulators and traditional banks to scramble to catch up and adapt to the evolving technology. [See "Banks Tried to Kill Crypto and Failed. Now They're Embracing It (Slowly)," by Emily Flitter, The New York Times, Nov. 1, 2021, tinyurl.com/zj4vpmnn, and "Wall Street Is Offering Big Pay Increases to Amass a Crypto Army," by Zijia Song and Katherine Doherty, Bloomberg, Nov. 1, 2021, tinyurl.com/mud3ye4k.]

Many organizations, however, are struggling to understand their digital asset exposure as dealing in crypto isn't immune to fraud risks. The large number of outstanding cryptocurrencies — 6,826 as of October 2021, up from just 66 in 2013 — and the general populace's lack of understanding about the technology opens opportunities for fraudsters. Indeed, the rapidly evolving nature of the digital asset ecosystem warrants strong compliance, legal and consumer protection controls. (See "Number of cryptocurrencies worldwide from 2013 to October 2021," by Raynor de Best, statista, Oct. 11, 2021, tinyurl.com/59m9psww, and "Cryptocurrencies, Digital Dollars, and the Future of Money," by Anshu Siripurapu, Council

on Foreign Relations, Sept. 24, 2021, tinyurl.com/yvs8enst.)

Appropriately, the opening message to the U.S. Department of Justice's 2020 "Cryptocurrency Enforcement Framework" (also referred to as the DOJ Framework; see tinyurl.com/syv474) reads, "Innovation can drive a society forward. But innovation does not occur in a vacuum. Public policy can establish background conditions that help the innovative spirit thrive — or create an environment in which that spirit is inhibited, or suppressed. Even in societies where transformative scientific and technological advancements are achievable, public policy again plays a critical mediating role. In the wrong hands, or without appropriate safeguards and oversight, these advancements can facilitate great human suffering."

Governments should also be prudent with their regulating authority and thoroughly understand the technology before attaching rules that may inhibit innovation or restrict consumers.

Defining crypto and its uses

Enthusiastic proponents of the blockchain or distributive ledger technology that supports and helps build cryptocurrencies say it has the potential to disrupt a number of industries that rely on middlemen and will make a world of difference in how we carry out commercial transactions. (See "How Blockchain Could Disrupt Banking," CBInsights, Feb. 11, 2021, tinyurl.com/5ebpw5v5.) Blockchain is sure to disrupt many traditional business services and industries such as accounting (think audits that require independent validation of financial statements), law (consider the complexity of contracts and validating signatures), and shipping and logistics (where certain events must happen within the supply chain before sending payment).

"With distributed ledger technology like Bitcoin, mortgages could process in three days as opposed to three months," says Keith Laska, a board observer at Uptick.co, a company that democratizes trading data insights for the crypto economy. "Employment verification will be instantaneous and irrefutable."

While different from cryptocurrencies, non-fungible tokens — digital proof of ownership of an authentic one-of-kind asset — is another offshoot of blockchain technology that many see as potentially revolutionizing the sale of everything from art to real estate. (See "Hot-ticket tokens, by Mason Wilder, CFE, *Fraud Magazine*, November/December 2021 issue, tinyurl.com/4r7avfpu.)

"Everything from real estate to intellectual property to sneakers and money will be tokenized," says Laska. "Tokenization enables faster and cheaper transactions through automation and smart contracts, providing (potentially) more transparency and accessibility."

Laska believes companies that proactively seek to understand and adopt these technologies will leapfrog ahead of their competitors. He is currently integrating Bitcoin acceptance into several of his companies, and strongly believes that over-regulation can stifle a once-in-a-generation technology transformation. "Bitcoin has handed us the 21st century's industrial revolution on a plate," he says. "We should embrace it and look for creative ways to simplify business processes as a result."

However, many of crypto's central features — including decentralized operation and control, and, in some cases, a high degree of anonymity — make it a perfect environment for fraudsters. This presents new and unique challenges that businesses, regulators and consumers must address, lest the technology be used predominantly for criminal activity.

Three categories of fraud risk

The DOJ Framework describes crypto's three primary fraud risk areas as follows: (See "Cryptocurrency Enforcement Framework," DOJ, October 2020, tinyurl.com/syv474.)

1. **Using cryptocurrency directly to commit crimes or to support terrorism.** Criminals use cryptocurrency to facilitate crimes and to avoid detection in ways that would be more difficult with fiat currency or "real money." They can avoid large cash transactions and mitigate the risk of bank accounts being traced, or of banks notifying governments of suspicious activity. Criminals have used cryptocurrency, often in large amounts and transferred across international borders, as a new means to fund criminal conduct ranging from child exploitation to terrorist fundraising. Cryptocurrency also has been used to pay for illegal drugs, firearms, and tools to commit cybercrimes, as well as to facilitate sophisticated ransomware and blackmail schemes.
2. **Using cryptocurrency to hide financial activity.** In addition to being used directly in transactions to commit crime or to support terrorism, bad actors also use cryptocurrency to hide and to promote financial activities attendant to unlawful conduct.
3. **Committing crimes within the cryptocurrency marketplace itself.** In addition to offering a means to commit old crimes in new ways, cryptocurrencies and the platforms on which they operate have often themselves become the target of criminal activity. To protect future victims, as well as to safeguard the integrity

"Committing appropriate resources with sufficient digital asset-specific experience and qualifications is key to implementing and monitoring fraud-related control activities," says Michael Carter chief compliance officer of Bittrex, Inc.

of cryptocurrency technology, more must be done to promote security and combat criminal activity on digital exchanges and platforms.

Fraud risk assessments: What should they cover?

Michael Carter, chief compliance officer of Bittrex, Inc., a leading cryptocurrency exchange, offers some advice to CFEs in the context of fraud risk management principles when adopting digital assets. He suggests that prior to any strategic pivot to a digital asset-based model or incorporation of cryptocurrencies for payment facilitation, a company should identify specific risks and implement appropriate controls into their larger fraud risk assessments. "Committing appropriate resources with sufficient digital asset-specific experience and qualifications is key to implementing and monitoring fraud-related control activities," Carter says.

In October 2018, the National Institute of Standards and Technology (NIST) published "NISTIR 8202: Blockchain Technology Overview" that can be synchronized with any organization's technical evaluation of blockchain-related fraud risks. (See tinyurl.com/4fpcdard.) According to Carter, organizations should understand both the common and unique fraud-related risks digital assets present, including:

- Technical stability and structure — Is the blockchain permissioned? Is it proof-of-work, proof-of-stake, or some other consensus mechanism? How are we securing and granting access to keys or signatures? (See "Proof of Work vs Proof of State," by Deborah Dobson, International Legal Technology Association, April 27, 2017, tinyurl.com/3zk25pka)
- Auditability — How does the blockchain enable auditing the value chain or financials, and how transparent and accessible should that be within the company?
- Hacking and theft — How secure is the network and who controls it? Is it vulnerable to coordinated attack or excessive downtime?
- Cyberattacks — How do we mitigate the risk of malicious users both internally and externally? How do we address altered chains, spoofing and diversion (theft)?
- Resource usage — Is the blockchain resource-intensive, requiring excessive participants and potentially more oversight?
- Financial reporting — How will tokenization affect the ability to appropriately report business income, financial health, and asset values?
- Even if you're not utilizing digital assets themselves, assessing secondary exposure to digital assets should be included in product, customer, service provider and vendor assessments.
- Economic purpose — What's the underlying economic purpose or utility of the cryptocurrency? Is it an additional asset to your balance sheet? Is it a faster method of transfer for value to/from businesses or consumers? Does it serve as a securitization of some other asset or is it just being used as a commodity? Understanding digital asset technology and how it affects the organization is important, but the fundamentals of combatting fraud remain the same.

Staying current

As CFEs, knowing the right business risk questions to ask is one of our professional hallmarks. While organizations and consumers continue to adopt crypto into their daily activities, as well as create new applications and use cases for blockchain technology, it's important that we stay abreast of leading guidance and fraud risk considerations so we can advise our stakeholders accordingly. Crypto is not going anywhere – we can be certain of that now. So let's make sure we have a seat at the table by staying current on leading trends and regulations.

Vincent M. Walden, CFE, CPA, is a managing director with Alvarez & Marsal's Disputes and Investigations Practice and assists companies with their anti-fraud, investigation and compliance monitoring programs. He welcomes your feedback, and would also like to thank his colleagues Larry Iwanski, Peter Kwan, Louis Konig, Jeremy Tilsner, Robert Johnson and Mark Kindy for their collaboration on this article. Contact Walden at vwalden@alvarezandmarsal.com.