New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 259—NO. 42
MONDAY, MARCH 5, 2018

OUTSIDE COUNSEL

Expert Analysis

Know Your Cryptocurrency: Traditional Due Diligence in a Disrupted World

BY DAVID BITKOWER,
MICHAEL ROSS
AND EMILY BRUEMMER

Cryptocurrency

Unless you've been living under a stack of savings bonds from the 1980s, you've seen news of the Bitcoin mania that's swept the financial world. As new entrants flood the market, speculation abounds that Bitcoin and other virtual currencies will usher in a new paradigm for the exchange of monetary value uncoupled from government backing—and that those currencies will eventually displace more traditional financial channels and intermediaries. That enthusiasm for cutting-edge currencies has been rivaled only by the frequent reports of fraud and abuse besetting those drawn to the new technology. Regulators including the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) have sounded the alarm that the virtual currency frontier is a digital Wild West.

What's most notable about the cloud over cryptocurrency, however, may be just how old-fashioned these threats are. The SEC has alleged that purported initial coin offerings (ICOs) from REcoin and Diamond Reserve Club were simply fancy fraud schemes based on empty promises. The CFTC has brought actions against other purported cryptocurrency investment opportunities, charging that they were little more than Ponzi schemes or similar deceptions. And last month a New York City man was held up at gunpoint in a plot to steal his digital wallet, which contained $1.8 million in Ether.

> What's most notable about the cloud over cryptocurrency may be just how old-fashioned these threats are.

But just as some of yesterday's abuses have surfaced in the digital era, so too can tried-and-true safeguards help protect against those abuses. Specifically, payment platforms or exchanges interfacing with cryptocurrencies or ICO tokens will be well served by drawing on familiar principles of due diligence, as long as they are thoughtfully applied with an eye toward the

DAVID BITKOWER *is a partner at Jenner & Block, where he is a member of the firm's investigations, compliance and defense practice.* MICHAEL ROSS *is a litigation partner in the firm's complex commercial litigation and securities litigation groups.* EMILY BRUEMMER *is an associate in the investigations, compliance and defense group.*

particular risks presented by the new technology and its uses.

This article highlights two recent cases to illustrate that point: (1) the SEC's recent enforcement action against the PlexCoin ICO, and (2) enforcement actions by DOJ and the Financial Crimes Enforcement Network (FinCEN) against virtual currency exchange BTC-e and its proprietor. These cases provide a useful opportunity for companies in the cryptocurrency space to consider the types of steps they should be taking to ensure that bad actors don't abuse their platforms.

The PlexCoin Case

On Dec. 1, 2017, the SEC's newly established Cyber Unit filed a complaint against a Canadian entity called PlexCorps and two individuals, principal Dominic Lacroix and business associate Sabrina Paradis-Royer, alleging that the company was defrauding investors through the issuance of "PlexCoins" or "PlexCoin Tokens" in a scam masquerading as an ICO. According to the complaint, the so-called ICO was premised on a series of misrepresentations, including the "outlandish" claim that investors would receive a return of 1,354 percent in less than 29 days. Lacroix and Paradis-Royer had already been enjoined from engaging in the offering by the Québec Financial Markets Administrative Tribunal, which had also issued orders against Lacroix on previous occasions.

As alleged in the complaint, Lacroix and Paradis-Royer offered PlexCoins to prospective investors in exchange for payment by credit card, over online payment platforms, or in virtual currencies such as bitcoin or Ether. The defendants then set up accounts on various platforms (such as PayPal, Shopify, and Stripe). In all, the defendants opened nearly half a dozen accounts on these platforms, listing different personal and entity names, contact information, and business purposes. Each account accepted funds for a short period of time until the relevant payment processor identified the account as problematic and shut it down. Ultimately, Lacroix and Paradise-Royer received more than $3.5 million in fiat currency from victims. But blockchain records and marketing materials indicate that the defendants may have sold more than $15 million worth of PlexCoins overall, suggesting that the bulk of investor payments were through other means, possibly through transactions involving cryptocurrencies. The SEC action seeks to enjoin further offerings, freeze any assets, and levy penalties.

> Companies entering the virtual currency space or otherwise interacting with virtual currencies and ICOs should recognize that many of the threats they face are really traditional frauds in technoclothing, and the best safeguards will often be the traditional ones that the financial sector has long relied on.

The BTC-e Case

In July 2017, several months before the PlexCorps case was brought, the Department of Justice (DOJ) unsealed a criminal indictment charging virtual currency exchange BTC-e and its principal, Alexander Vinnik, with offenses involving money laundering and operating an unlicensed money services business. Simultaneously, FinCEN fined BTC-e and Vinnik for failing to comply with the U.S. anti-money laundering (AML) framework applicable to money transmitters. The indictment alleged that, despite transmitting value to and from customers in the United States, BTC-e was not properly registered as a money services business and also "lacked basic anti-money laundering controls and policies" and "Know Your Customer" policies required by law for money transmitters. For instance, BTC-e collected "virtually no customer data at all," only requiring a username and email address for sign-up. It also required users to make transactions through third-party exchangers, rather than through BTC-e itself, and thus avoided the creation of a "centralized financial paper trail." As a result, BTC-e was allegedly able to serve as a "money-laundering enterprise"—as the "exchange of choice to convert digital currency like bitcoin to fiat currency for the criminal world." The indictment alleged that the exchange attracted criminal proceeds from crimes such as identity theft, tax fraud, public corruption, drug trafficking, ransomware, and computer hacking—including the notorious hacking of virtual currency exchange Mt. Gox.

As one means of identifying the criminal nature of the exchange's activities, government investigators turned to the blockchain—the distributed public ledger of all bitcoin transactions. Investigators were able to use it to trace a portion of the bitcoin spirited away from Mt. Gox to ultimate destinations in BTC-e accounts and Vinnik himself. According to the indictment, of the 530,000 bitcoin stolen from Mt. Gox, 300,000 bitcoin went directly to three BTC-e accounts, which were linked to each other, and in turn to accounts controlled by BTC-e administrators, including Vinnik. Additional funds from the hack were deposited in another bitcoin exchange and back into Mt. Gox itself, but each time to accounts that

could be linked to a Vinnik-controlled account at BTC-e. In short, the available record of bitcoin transactions linked BTC-e, and Vinnik, to specific prior criminal conduct—ultimately contributing to the indictment of both for money laundering and the FinCEN penalty.

A New Context, But Traditional Safeguards

As these examples illustrate, the successes of virtual currencies, like those of many new technologies, have been accompanied by unscrupulous schemes to exploit the public and legitimate businesses. At the same time, though, the examples illustrate that not all tech-savvy criminals are criminal masterminds, and that you don't necessarily need to be a cryptography expert to protect yourself. Indeed, one lesson that the raft of cryptocurrency-related crimes and enforcement actions hold is that traditional safeguards can help guard against victimization and abuse.

For example, some of the flags that were raised by Lacroix's and Paradis-Royer's account activities were exactly those that financial institutions have had long experience watching for. Each of the accounts received a large influx of deposits in a short period of time. They had reported vague business purposes in opening their accounts—either "PlexCoin" or "SidePay"—and an Internet search could have linked those names to promotional materials for the scheme, and potentially to the Canadian administrative order enjoining it. At least one account was opened in Lacroix's name despite his criminal record in Canada and the more recent Canadian injunction. Presumably as a result of these or similar flags, the payment platforms cited in the Complaint all ultimately suspended the accounts. PayPal, for example, "[a]lmost immediately" flagged Lacroix's account for suspicious activity and "reversed most of the payments to the investors."

Those familiar safeguards may require new applications when it comes to virtual currencies. As the BTC-e case highlights, virtual currencies are generally pseudonymous, and transactions are thus not always clearly linked to identifiable individuals. Despite that feature, the public blockchain that underlies bitcoin and other virtual currencies creates a reviewable record of every transaction. That record, therefore, permits analysts to trace transactions through time and attempt to tie historical crimes to present-day wallets, even without the identity of the individuals behind them. In the BTC-e case, law enforcement agencies were able to trace proceeds from the Mt. Gox hack directly to BTC-e accounts, just as they have been able to trace dirty bitcoin in other cases, such as the investigation of Ross Ulbricht, the convicted administrator of the Silk Road dark marketplace. Research has demonstrated both the possibilities of this type of due diligence and some of its limits.

For regulated businesses, such steps to trace transactions may increasingly be seen as requirements as regulators step up scrutiny over virtual currency businesses. Those laws and regulations require that money transmitters register with the Treasury Department and individual states where they do business, and maintain an "effective" AML program that includes internal policies, procedures, and controls tailored to the risks associated with the business. The precise contours of what an effectively tailored AML program means in the cryptocurrency context remain to be fleshed out, and the policies and procedures a company adopts will have to be commensurate with the precise risks it faces. But reasonable steps to take advantage of the features of the new technology are an example of the type of traditional due diligence that regulators are likely to begin to expect from companies, depending on their risks and other controls.

* * *

Recent history has shown that the challenge posed by virtual currency is not to reconceive compliance, but rather to apply familiar concepts to a new context. Companies entering the virtual currency space or otherwise interacting with virtual currencies and ICOs should recognize that many of the threats they face are really traditional frauds in techno-clothing, and the best safeguards will often be the traditional ones that the financial sector has long relied on. In the specific context of virtual currencies, that may entail a greater focus on fly-by-night grifts and scrutiny of anonymity-seeking or border-hopping customers. By the same token, it may also mean taking advantage of the historical record the blockchain provides, and the ability to find digital red flags out in the open. Regulated businesses in particular should be aware that government investigators are using those techniques to unravel digital fraud schemes, and may in some cases ask whether a business could have done so as well.

In recent months, much of the most high profile enforcement attention has been on the alleged bad actors who are abusing others' enthusiasm for new technology for their own criminal ends. But, as the SEC's recent subpoenas suggest, the focus of regulators will inevitably broaden, and responsible participants in the marketplace should be thinking carefully about taking reasonable steps to prevent the abuse of their platforms before it does.