The following article is from National Underwriter's latest online resource,
FC&S Legal: The Insurance Coverage Law Information Center.

FC&S LEGAL
The Insurance Coverage Law Information Center

AT THE END OF YOUR TETHER: ADDRESSING, RESPONDING TO, AND INSURING CRYPTOCURRENCY THEFT

January 17, 2018

Herbert F. Kozlov, J. Andrew Moss, Kari S. Larsen, Vincent James (Jim) Barbuto

Tether, the company behind USDT – a digital token backed by fiat currencies like the dollar and euro – disclosed that a hack resulted in the loss of $30.95 million worth of tokens.[1] Tether posted an announcement to its website November 19, 2017 reporting that a "malicious action by an external hacker" resulted in the coins being "removed from the Tether Treasury wallet" and "sent to an unauthorized Bitcoin address."[2] Tether worked to "blacklist" or otherwise inhibit hackers from using the stolen coins following the hack.

The Tether hack illuminates the privacy, reputational, financial and recovery risks associated with issuing, owning, and storing digital currencies. These risks and events are likely to repeat themselves as more initial coin offerings ("ICO") come to the market, and the prices of digital currencies continue to soar.

According to Tether, USDT tokens are pegged to fiat currency to decrease the volatility experienced by non-fiat backed cryptocurrencies, such as Bitcoin, and to facilitate trading of USDT tokens on crypto-exchanges.[3] Although it is a less commonly used coin, the Tether hack rippled throughout the cryptocurrency market. News of the Tether theft contributed to a 5.4 percent decline in Bitcoin's value the week the incident was announced (it eventually recovered).[4]

Background: Recent Breaches/Cryptocurrency Thefts and the Consequences

Tether is only the most recent of a number of security incidents that have befallen cryptocurrency providers and partners since the introduction of Bitcoin in 2009. Although the Bitcoin blockchain (the underlying distributed ledger of the digital currency) itself is often touted as unhacked (as of yet), a litany of digital wallets (resources for users to store cryptocurrencies), cryptocurrency exchanges, and ICOs have suffered losses to hackers, often without realistic recourse for issuers or users who have incurred significant losses.

Two of the largest cryptocurrency exchanges, Bitfinex and Coinbase, have both been targeted by hackers, as have the digital wallets of their customers. Last year, Bitfinex suffered the second-largest exchange platform breach, resulting in the loss of $72 million in users' Bitcoin from the exchange.[5] The exchange later reimbursed affected customers.[6] The U.S. Commodity Futures Trading Commission ("CFTC") also fined the exchange "for offering illegal off-exchange financed retail commodity transactions,"[7] by offering trades on margin and not "actually delivering" the cryptocurrencies within the required timeframe of 28 days.[8] The CFTC considered the exchange's security and access controls in its analysis, and determined that by controlling the private keys that accessed customers' digital wallets, Bitfinex was interfering with the level of "possession and control" required to connote "actual delivery" under the Commodity Exchange Act.[9] Tether and Bitfinex share an owner,[10] and their relationship, coupled with continued security vulnerabilities, including a distributed denial-of-service ("DDoS") attack on the exchange as recently as November 26,[11] have fueled speculation and accusations surrounding the Tether hack.[12]

Coinbase, a cryptocurrency exchange valued at more than $1 billion,[13] has also experienced multiple wallet-based incidents whereby hackers exposed vulnerabilities to the Signaling System 7 (SS7) to manipulate customers' SMS-based, two-factor authentication wallet access systems and drain coins from their accounts, sometimes before their eyes.[14] According to reports, "hackers have never breached Coinbase's own virtual fortress,"[15] but the exchange's security has not prevented significant losses from customers' accounts.

The risks associated with cryptocurrency operations do not stop at the issuer's or exchange's doorstep; massive losses can occur from issues systemic to the on-ramps and off-ramps used to access, trade, and store digital currencies on a distributed network.[16]

In July 2017, $30 million in Ether was stolen when hackers exploited vulnerabilities in a startup's digital wallet to obtain exclusive ownership of the wallet and move all of its funds.[17] Attempts to fix the bug in November may have unintentionally frozen (effectively lost) an additional $150 million or more in an irreversible transaction, highlighting one way in which blockchain technology's immutability (typically an advantage for transactional transparency and recordkeeping) can have disastrous consequences.[18]

ICOs have also become targets for cryptocurrency theft. Last summer, trading platform CoinDash tried to take advantage of the growing trend of selling digital tokens as a method to raise capital, but after only 13 minutes, hackers diverted between $7 million and $10 million of investor capital away from the ICO before CoinDash could put a stop to it.[19]

In June 2016, between $55 million and $67 million in Ether were stolen from an Ethereum-based venture capital fund known as the DAO, a particular Decentralized Autonomous Organization on the network, which put a further $250 million at risk and resulted in a "hard fork" (a radical protocol change that alters the validity of previous blocks in a chain) of the Ethereum blockchain to contain the losses.[20] Liability for this incident was unclear at best, given that the DAO was stateless and lacked a traditional corporate structure to indicate under what jurisdiction incidents should fall and who should be liable.[21]

In the wake of these and many other incidents, regulators, issuers and investors have been struggling to build a framework around which this new financial technology can function safely. For starters, the U.S. Securities and Exchange Commission ("SEC") has issued guidance clarifying that some token sales are subject to U.S. securities laws.[22] This interpretation and the resulting examination of ICOs under the *Howey* securities test has increased the risk that digital asset issuers could be subject to regulatory scrutiny and securities class action litigation, some of which have already begun.[23] As such, the risks inherent to transacting in this space have not been fully addressed, particularly with respect to cybersecurity and financial recovery, both of which are key to the preparedness for and responsiveness to incidents such as those outlined above.

Cryptocurrency (and Blockchain) Cybersecurity

From a cybersecurity perspective, and as discussed above, the immutability, encryption, and cryptographic elements inherent in cryptocurrency transactions on a blockchain can lend themselves well to a secure environment. Cryptocurrencies and other blockchain applications can provide added security by inhibiting tampering and distributing data across all the nodes of a network (rather than a single target server/a single point of failure for a DDoS attack), and they can mitigate traditional access control risks through the use of public and private key infrastructure to access encrypted data and prevent a hacker from destroying a network (or holding it for ransom) through one unauthorized access point.[24]

Despite the added security benefits of cryptocurrencies' underlying blockchain technology, external pressures and threats pose risks that require an up-front assessment of vulnerabilities and countermeasures. Notably, off-chain entry and exit points (on-ramps or off-ramps) to a distributed cryptocurrency ledger, and the mechanisms by which digital currencies are stored (like the digital wallets hacked in the examples above, or the loss of private keys), introduce penetration points that can capitalize on the blockchain's irreversibility, whereby pilfered digital tokens and coins cannot be returned, and victims can be left without much recourse (unless issuers and users are properly insured or indemnified). Similarly, the use of private and public key authentication on a distributed network can create risk with respect to users' private keys that, if lost or compromised, can result in serious losses.

The rapid evolution of data protection regulations will impact security for cryptocurrencies and on blockchains generally. The European Union's Global Data Protection Regulation (GDPR), in particular, focuses significantly on who controls and who processes data. A question still exists as to the interplay between the European "right to be forgotten" and the inability to execute the deletion of data on a blockchain. The concepts paramount to many data privacy and security laws do not align cleanly with the decentralized and immutable components of blockchain technologies, and may require enhanced security features to be built on top of existing cryptocurrency frameworks to be compliant.[25] The lack of clarity surrounding remedies and recourse for incidents similar to those outlined above, coupled with the potential for class actions against cryptocurrency issuers (especially where the digital coin would be considered to be securities[26]), highlights the risks that issuers, exchanges, and users of cryptocurrencies face, and the need for adequate insurance solutions to account for these risks.

Financial Recovery for Losses: Insurance and Underwriting Issues

Cryptocurrencies do not require financial institutions to issue them or banks to store them. Because transactions generally are non-reversible and may be anonymous, the risks of financial loss increase.

Traditional insurance coverage, such as network security and privacy liability ("cyberliability") insurance, financial institution bonds and commercial crime insurance, directors' and officers' liability ("D&O") insurance, and professional liability errors and omissions ("E&O") insurance, all should be considered as part of a cryptocurrency insurance program.

More specifically, insurers have developed insurance products to address both the traditional risks associated with the financial services industry and the unique and emerging aspects of cryptocurrencies. Cyberliability insurance is intended to address first-party losses and third-party liability as a result of data security incidents, the disclosure of or failure to protect private information, and privacy law violations. Some cryptocurrency exchanges and wallet providers have partnered with traditional insurers and brokers to place and offer tailored coverage for the direct loss of cryptocurrency because of digital wallet theft as a result of a breach to the wallet provider, such as from hacking or physical theft through a breach of provider cold storage, or employee theft or fraud.[27] Currently available cryptocurrency insurance products should be carefully reviewed. Like all insurance policies, cryptocurrency insurance products contain exclusions and terms and conditions that may affect recovery. For instance, cryptocurrency-specific policies may exclude loss as a result of a breach of the wallet owner/user's own security. Cryptocurrency-specific policies may only provide coverage under narrow factual circumstances, such as crime and employee misconduct,[28] whereas others may broadly cover the risk of loss both to the exchange as a policyholder and to exchange customers.[29] Just as the risks associated with data security and privacy liability are continuing to evolve, cyberliability insurance policies are an evolving product and are not standardized, and should be reviewed carefully. Policies should be drafted to insure against liability related to the company's storage or exchange of digital currency, the corruption or breach of its associated technology, or losses as a result of a compromised vendor – each tailored to the relevant business. Cyberliability insurance also often covers cyber extortion in which payment is demanded in exchange for terminating a threat or an attack. "Ransomware" cyberattacks, which routinely demand payment in bitcoin or other digital currency in exchange for terminating the attack, should be included in cyber extortion coverage.

Financial institution bonds and commercial crime insurance cover direct losses of money, property, and securities as a result of specified dishonest and criminal acts by employees and outsiders. These policies should include coverage for losses directly caused by computer fraud and social engineering (phishing) fraud. In the absence of clearly defined coverage, token thefts resulting from compromised access information obtained via social engineering and phishing have resulted in refusals to pay claims by insurers and subsequent litigation to pursue recovery.[30] D&O insurance protects a company's directors and officers against third-party liability related to their management of the company, and also often covers the company itself for securities claims (some private company D&O coverage may apply to a broader scope of claims made against the company itself). Securities claims covered under D&O policies generally include actions alleging violations of federal, state or foreign laws and regulations governing securities issued by the insured company. Cryptocurrency operators, issuers or users should ensure that their policies will cover securities lawsuits arising from registration issues or alleged misrepresentations to contributors or investors in an initial coin offering, a loss of coins, or damage to the operations sustained by a wallet or other vulnerability.

Finally, issuers should consider E&O insurance, which is designed to protect from third-party liability for professional errors and omissions. E&O polices can be tailored to specific professions and risks, and are frequently negotiable. A number of insurers appear to have developed tailored cryptocurrency products, which may also incorporate cyberliability coverage and commercial crime protection, but have yet to arrive at a comprehensive solution.[31] Other companies have created captive insurance funds to protect their customers instead of turning to insurance companies.[32]

Conclusion

As the technology evolves, so will the crime associated with exploiting its vulnerabilities. Technology, regulatory, and insurance coverage counsel can assist policy holders, issuers, and users to navigate these and other related issues both during attempts to obtain insurance coverage and after any losses occur. An ounce of prevention is often worth a pound of cure, but if not possible, insurance may address some of the cure.

Notes

[1]. *CNBC, More than $30 million worth of cryptocurrency was just stolen by hackers, company says*, Nov. 21, 2017, https://www.cnbc.com/2017/11/21/tether-hack-attacker-reportedly-steals-30-million-of-digital-tokens.html.

[2]. Tether, Tether Critical Announcement, Nov. 21, 2017, https://tether.to/tether-critical-announcement/.

[3]. Tether, *FAQs*, Nov. 22, 2017, https://tether.to/faqs/.

[4]. Price volatility raises issues with the financial strength of insured companies, the severity of the risks they face, and how to predict or quantify losses; *see* generally TechCrunch, *Tether, a startup that works with bitcoin exchanges, claims a hacker stole $31M,* Nov. 20, 2017, https://techcrunch.com/2017/11/20/tether-claims-a-hacker-stole-31m/.

[5]. Fortune, *Can Bitfinex Really Impose a $72 Million Theft on Its Customers?* Aug. 15, 2016, http://fortune.com/2016/08/15/bitfinex-bitcoin-hack-hong-kong-customers-law/.

[6]. Cryptocoins News, *Bitcoin Exchange Bitfinex Completes Reimbursing Customers for 2016 Hack Losses*, https://www.cryptocoinsnews.com/bitfinex-completes-reimbursing-customers-for-hack-losses/.

[7]. U.S. Commodity Futures Trading Commission Press Release, June 2, 2016: "CFTC Orders Bitcoin Exchange Bitfinex to Pay $75,000 for Offering Illegal Off-Exchange Financed Retail Commodity Transactions and Failing to Register as a Futures Commission Merchant," *available at* http://www.cftc.gov/PressRoom/PressReleases/pr7380-16.

[8]. *Id.*

[9]. BFXNA Inc. d/b/a BITFINEX. Order Instituting Proceedings Pursuant to Sections 6(c) and 6(d) of the Commodity Exchange Act, as amended, Making Findings and Imposing Remedial Sanctions. CFTC Docket No. 16-19, June 2, 2016, http://www.cftc.gov/idc/groups/public/@lrenforcementactions/documents/legalpleading/enfbfxnaorder060216.pdf; *see also* CFTC v. Hunter Wise Commodities LLC, 749 F.3d 967, 978-79 (11th Cir. 2014).

[10]. Nathaniel Popper, *Warning Signs about another Giant Bitcoin Exchange*, New York Times (Nov. 21, 2017), https://www.nytimes.com/2017/11/21/technology/bitcoin-bitfinex-tether.html.

[11]. Rachel McIntosh, *Bitfinex on Twitter: Exchange is Under DDoS Attack; Question Arise*, Finance Magnates (Nov. 27, 2017), https://www.financemagnates.com/cryptocurrency/exchange/bitfinex-twitter-exchange-ddos-attack-question-arise/.

[12]. Kai Sedgwick, *Questions Mount as Bitfinex Stay Silent in the Wake of the Tether Hack*, Bitcoin.com (Nov. 22, 2017), https://news.bitcoin.com/questions-mount-bitfinex-stay-silent-wake-tether-hack/.

[13]. Robert Hackett, Fortune, *Coinbase Becomes First Bitcoin 'Unicorn'* (Aug. 10, 2017), http://fortune.com/2017/08/10/bitcoin-coinbase-unicorn/.

[14]. Nathanial Popper, *Identity Thieves Hijack Cellphone Accounts to Go After Virtual Currency*, New York Times (Aug. 21, 2017), https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html; Fortune, Cryptocurrency Exchanges Are Increasingly Roiled by Hackings and Chaos (Sep. 29, 2017), http://fortune.com/2017/09/29/cryptocurrency-exchanges-hackings-chaos/.

[15]. Jen Wieczner, *Hacking Coinbase: The Great Bitcoin Bank Robbery,* Fortune (Aug. 22, 2017), http://fortune.com/2017/08/22/bitcoin-coinbase-hack/.

[16]. *Id.*

[17]. Wolfie Zhao, *$30 Million: Ether Reported Stolen Due to Parity Wallet Breach*, Coindesk (Jul. 19, 2017), https://www.coindesk.com/30-million-ether-reported-stolen-parity-wallet-breach/.

[18]. Ryan Browne, *Accidental' bug may have frozen $280 million worth of digital coin ether in a cryptocurrency wallet*, CNBC (Nov. 8, 2017), https://www.cnbc.com/2017/11/08/accidental-bug-may-have-frozen-280-worth-of-ether-on-parity-wallet.html; *see also* Alex Hern, *'$300m in cryptocurrency' accidentally lost forever due to bug*, The Guardian (Nov. 8, 2017), https://www.theguardian.com/technology/2017/nov/08/cryptocurrency-300m-dollars-stolen-bug-ether.

[19]. Jen Wieczner, *Hackers Just Stole $7 Million in a Brazen Ethereum Cryptocurrency Heist*, Fortune (Jul. 18, 2017), http://fortune.com/2017/07/18/ethereum-coindash-ico-hack/.

[20]. Jan Vollmer, *The Biggest Hacker Whodunnit of the Summer*, Motherboard (Jul. 16, 2016), https://motherboard.vice.com/en_us/article/pgkzqm/the-biggest-hacker-whodunnit-of-the-summer; *see also* Matthew Leising, The Ether Thief, Bloomberg (June 13, 2017), https://www.bloomberg.com/features/2017-the-ether-thief.

[21]. Tanaya Macheel, *The DAO Might Be Groundbreaking, But Is It Legal?* American Banker (May 19, 2016), https://www.americanbanker.com/news/the-dao-might-be-groundbreaking-but-is-it-legal.

[22]. U.S. Securities and Exchange Commission Press Release, July 25, 2017: "SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities," *available at* https://www.sec.gov/news/press-release/2017-131; *see also* https://www.fintechupdate.com/2017/11/cftc-and-sec-chairs-seek-to-apply-existing-laws-and-regulations-to-digital-assets/.

[23]. Anna Irrera, *Tezos organizers sued in California over crypto currency project*, Reuters (Nov. 3, 2017), https://www.reuters.com/article/us-bitcoin-tezos-battles/tezos-organizers-sued-in-california-over-crypto-currency-project-idUSKBN1D325A.

[24]. Jill Richmond, *Advancing Cybersecurity with Blockchain Technology*, NASDAQ (Apr. 26, 2017), http://www.nasdaq.com/article/advancing-cybersecurity-with-blockchain-technology-cm780007.

[25]. Jacek Czarnecki, *Blockchains and Personal Data Protection Regulations Explained*, Coindesk (Apr. 26, 2017) https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/.

[26]. Sophia Morris, *Tezos Hit with Class Suit over Cryptocurrency Offering*, Law360 (Nov. 27, 2017), https://www.law360.com/articles/988251/tezos-hit-with-class-suit-over-cryptocurrency-offering.

[27]. *See* "Theft Insurance," https://www.circle.com/en-ie/legal/intl-user-agreement; *see also* https://support.coinbase.com/customer/portal/articles/1662379-how-is-coinbase-insured.

[28]. *See* https://www.businesswire.com/news/home/20140602006331/en/Great-American-Insurance-Group-Offer-Bitcoin-Coverage#.VYCmI89VhBf.

[29]. Luke Parker, *Insurance policy now available for bitcoin exchanges*, BraveNewCoin (Nov. 26.2016), https://bravenewcoin.com/news/insurance-polic-now-available-for-bitcoin-exchanges/.

[30]. *See Bitpay, Inc. v. Massachusetts Bay Ins. Co.*, 315 F.R.D. 698 (N.D. Ga. 2016).

[31]. Gautham, *BitGo Insurance Blog Taken down as Bitfinex Fiasco Continues*, NewsBTC (Aug. 4, 2016), http://www.newsbtc.com/2016/08/04/bitgo-bitfinex-hacking-fiasco/.

[32]. *See* https://support.xapo.com/insurance (last visited Oct. 7, 2015).

About the Authors

Herbert F. Kozlov (hkozlov@reedsmith.com) is a partner at **Reed Smith LLP** focusing his practice on corporate law.

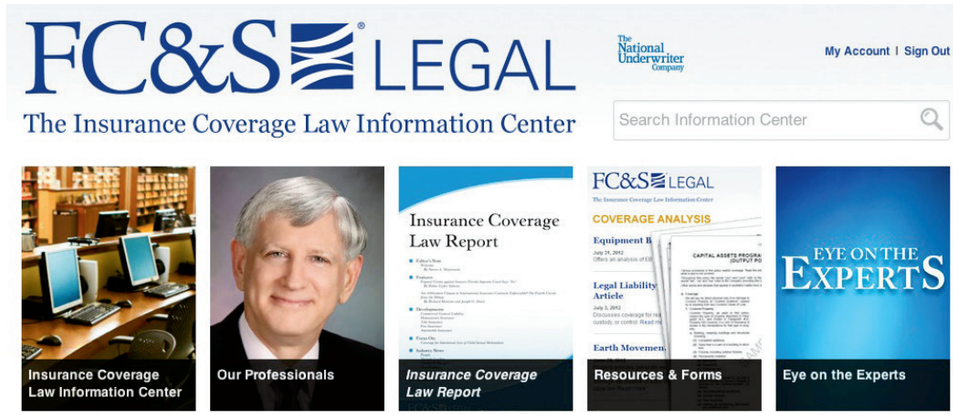
J. Andrew Moss (amoss@reedsmith.com) is a partner at **Reed Smith LLP** and a member of the Insurance Recovery Group.

Kari S. Larsen (klarsen@reedsmith.com) is counsel at **Reed Smith LLP** representing clients in regulatory, legislative, and transactional matters.

Vincent James (Jim) Barbuto (vbarbuto@reedsmith.com) is an associate at **Reed Smith LLP** in the firm's IP, Tech & Data Group.

***

This article appeared in the Winter 2018 issue of the *Insurance Coverage Law Report*.



For more information, or to begin your free trial:

- Call: 1-800-543-0874
- Email: customerservice@nuco.coms
- Online: www.fcandslegal.com

FC&S Legal guarantees you instant access to the most authoritative and comprehensive insurance coverage law information available today.

This powerful, up-to-the-minute online resource enables you to stay apprised of the latest developments through your desktop, laptop, tablet, or smart phone —whenever and wherever you need it.

NOTE: The content posted to this account from ***FC&S Legal: The Insurance Coverage Law Information Center*** is current to the date of its initial publication. There may have been further developments of the issues discussed since the original publication.