**Portfolio Media. Inc.** | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

# How Biden Administration Can Crack Down On Ransomware

By **John Stark** (January 12, 2021, 1:13 PM EST)

John Stark

Bitcoin has found its killer app in ransomware, a type of malicious software designed to block access to a computer system or computer files until an extortion demand is paid.

Ransomware attacks are the other plague of 2020, except with ransomware, there will never be a vaccine. No matter how sophisticated and vigilant, no company can ever enjoy immunity from a cyberattack. Cybersecurity remains an oxymoron.

But the situation is not as hopeless as it seems. Crucial to any successful ransomware scheme is collecting the ransom in pseudo-anonymous cryptocurrency, typically bitcoin. Disrupt the flow of bitcoin and ransomware attackers will have no means to anonymously, conveniently, expeditiously and securely collect their extortion demand. But how?

The answer is simple. By using the effective and novel prosecutorial tactic known as access theory, President-elect Joe Biden can initiate a 2021 prosecutorial offensive to stop ransomware. Access theory involves targeting the conduits and go-betweens, such as cryptocurrency financial platforms, custodian and wallet services and other intermediaries, that criminals use: (1) to trade and convert the bitcoin and any other cryptocurrency extorted from ransomware victims; and (2) to use to hide and launder ill-gotten gains.

Legal and cyber pundits alike often lament that the U.S. financial regulatory structure was not designed to tackle the technical complexities of cryptocurrency, harping on the disfunction and chaos created when no single federal agency wields comprehensive authority over its many varying elements. However, when it comes to tackling ransomware, cryptocurrency's jurisdictional maze and lack of precedent are actually strengths, not weaknesses.

In other words, even though the government can't prove that an unsafe and dangerous car has been involved in a hit-and-run, the government still has the tools to take that car off the road.

### What Is Access Theory?

Access theory originates from the prosecutorial playbook of the late U.S. District Judge Stanley Sporkin, who served as enforcement director at the U.S. Securities and Exchange Commission from 1974 to 1981 and championed gatekeeper liability, premised upon what he referred to as the access theory.

Sporkin's decree: Instead of pursuing every bad actor, take the easier road and pursue the gatekeepers who control access to U.S. capital markets. In the cryptocurrency marketplace, the most obvious targets for a gatekeeper assault include:

- Cryptocurrency platforms, including cryptocurrency exchanges,[1] which allow for the conversion of bitcoin and other cryptocurrencies into dollars;

- Cryptocurrency custodial services that provide digital wallet and other storage solutions; and

- Corporate cryptocurrency facilitators that manage transactions for retailors that accept cryptocurrency as payment.

**DOJ Enforcement**

The U.S. Department of justice seems especially well-suited to employ access theory as an anti-ransomware munition.

As indicated in its Oct. 8, 2020, Cryptocurrency Enforcement Framework,[2] the DOJ enjoys broad jurisdiction in order to combat cryptocurrency's substantial role in serious criminal activity. Potential federal criminal charges may arise from:

- Wire, mail and securities fraud;

- Tax fraud;

- Identity theft;

- Violating anti-money laundering, know-your-customer and combating-the-finance-of-terrorism requirements — or AML, KYC and CFT, respectively; and

- Operating an unlicensed money transmitting business, or MSB.

The framework reveals that the DOJ is expanding its focus to the entire cryptocurrency ecosystem, including trading platforms, crypto kiosks, virtual currency casinos, custodial and digital wallet providers, etc. The DOJ can prosecute each for failure to safeguard customer data and failure to stop their wares from exploitation by terrorists and money launderers.

**AML Regulation**

In the U.S., individuals and entities that offer money transmission or conversion services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers and brokers of virtual assets, are considered MSBs.

Like brick-and-mortar financial institutions, MSBs are subject to AML and CFT regulations as well as a range of substantial licensing and registration, which in turn could trigger civil liability, penalties, fines, license revocation even criminal prosecution. For instance, per the Financial Crimes Enforcement Network's 2013 guidance,[3] cryptocurrency service firms with unclean hands could face criminal charges for failure to:

- Register with FinCEN;
- Maintain an effective AML program;
- Comply with AML record-keeping requirements; and
- File with FinCEN suspicious activity reports regarding customers who use cryptocurrencies for unlawful purposes.

**MSB Regulation**

Federal and state prosecutors and regulators also enjoy a lesser known — and oft misunderstood — jurisdictional hook when cryptocurrency intermediaries run afoul with state registration of money transmitters.

A subset of the larger group of MSBs,[4] a money transmitter is typically defined to include a person that "provides money transmission services, or any other person engaged in the transfer of funds." The term "money transmission services" means "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[5]

Pursuant to Title 18 of the U.S. Code, Section 1960, titled Prohibition of Unlicensed Money Transmitting Businesses:

> Whoever knowingly conducts, controls, manages, supervises, directs, or owns all or part of an unlicensed money transmitting business, shall be fined in accordance with this title or imprisoned not more than 5 years, or both.[6]

As part of the USA Patriot Act, Congress amended Section 1960(b)(1)(A) to provide that a defendant can be convicted of operating an unlicensed money transmitting business "whether or not the defendant knew that the operation was required to be licensed or that the operation was so punishable."[7] This strict liability paradigm allows prosecutors to allege liability regardless of the perpetrator's intent or mental state.[8]

Importantly, FinCEN's requirements apply equally to domestic and foreign-located MSBs, even if the foreign-located MSB has no physical presence in the U.S.[9] The MSB need only do business in

whole or substantial part in the U.S. In addition, parties become money transmitters, and therefore MSBs, whether they exchange from fiat to convertible cryptocurrency or from one cryptocurrency to another cryptocurrency.

Given the anonymity preferences of cryptocurrency traders, meeting AML, KYC and Office of Foreign Assets Control responsibilities is a Herculean task for cryptocurrency firms, making charging decisions easier and providing compelling prosecutorial fodder.[10]

**SEC Regulation**

The SEC has already brought a slew of enforcement actions[11] addressing the typically bold[12] and transparent violations[13] of SEC regulations by cryptocurrency firms. The SEC could in 2021 redouble their efforts applying access theory.

For example, cryptocurrency intermediaries that offer digital wallet services and other crypto-custodial services may trigger registration requirements under U.S. federal securities laws, including broker-dealer, transfer agent, or clearing agency registration or may be participating in the unregistered offer and sale of securities.

In addition, per the SEC,[14] some cryptocurrency intermediaries that are directly or indirectly offering trading or other services related to digital assets that are securities, may have failed register as exchanges under the federal securities laws.

**IRS Enforcement**

When a U.S. taxpayer has traded cryptocurrency like bitcoin for a profit, a failure to pay the tax on that gain could be unlawful. By issuing subpoenas to cryptocurrency gatekeepers, the IRS can identify tax-delinquent U.S. taxpayers and disrupt the global cryptocurrency marketplace.

Along these lines, the IRS has issued subpoenas to several cryptocurrency trading platforms, ordering them to disclose details about user accounts.[15]

For example, in 2018, Coinbase Inc. had to disclose details relating to approximately 13,000 user accounts[16] pursuant to John Doe summonses.[17] Moreover, starting with the 2020 tax season, on the new Form 1040 Schedule 1, every taxpayer will need to declare whether they have or have not used cryptocurrency in one way or another.[18]

**The AMLA**

The U.S. Senate has now completed the override of President Donald Trump's veto of the National Defense Authorization Act and, as part of that legislation, passed the Anti-Money Laundering Act of 2020.[19] The AMLA has a range of provisions that could result in significantly increased civil/criminal enforcement against cryptocurrency firms for AML violations, including significantly expanding the AML whistleblower award program, which will be a real game changer.[20]

Specifically, the AMLA includes anti-retaliation protections for whistleblowers and mandates that when an AML enforcement action brought by the DOJ or the U.S. Department of the Treasury results in monetary sanctions over $1 million, the Treasury secretary "shall" pay an award of up to 30% of what was collected to whistleblowers who "voluntarily provided original information" that led to a successful enforcement action. The previous AML whistleblower award program limited awards in most cases to $150,000 and was discretionary.

It would be hard to overstate the far-reaching potential effects of this new program.[21]

Suddenly, there exists substantial rewards and robust protections for anyone coming forward with AML complaints relating to cryptocurrency intermediaries like trading platforms, exchanges, wallets, kiosks, etc.

Even compliance officers and internal auditors could collect substantial whistleblower awards. And the AMLA not only incentivizes U.S. tipsters — foreign nationals who work for cryptocurrency intermediaries operating beyond U.S. borders are also eligible for whistleblower awards.

The AMLA also expands the definition of financial institution and money transmitting business to include businesses engaged in the exchange or transmission of "value that substitutes for currency," potentially reinforcing the government's position that the Bank Secrecy Act applies to cryptocurrency. In addition, the AMLA adds resources for additional AML federal investigators and experts:

- Establishing special hiring authority for FinCEN and the Office of Terrorism and Financial Intelligence;[22]

- Creating FinCEN domestic liaisons to oversee different regions of the U.S., as well as Treasury attachés and FinCEN foreign intelligence unit liaisons to be stationed at U.S. embassies or foreign government facilities;[23] and

- Creating a subcommittee on innovation and technology to advise the secretary of the Treasury on innovation with respect to AML and calls for BSA innovation officers and information security officers at FinCEN and other federal financial regulators.[24]

Given the potential for AML deficiencies at the many cryptocurrency firms that provide one-stop money laundering services for ransomware attackers, the AML whistleblower program will undoubtedly spawn an army of lawyers and consultants who will flesh out cryptocurrency whistleblowers and ensure the proper disposition of their complaints.

**A Biden Cryptocurrency Crackdown**

The success of ransomware attacks has bred a global criminal ecosystem of large and sophisticated cybercriminal organizations that now provide the tools, training and ability to collect ransoms, reducing the need for bespoke cyberattacks and malware coding.

Moreover, the threat is no longer merely the kidnapping of data but also the public release of that data via social media. Ransomware attackers have even sharpened their business models, including guaranteeing turnaround times, providing real-time chat support for victims, and offering payment demands customized to a victim's financial profile.

Meanwhile, threat actors associated with rival nations such as Iran and North Korea have adopted ransomware attacks as a fast and easy means to bypass U.S. economic sanctions and funnel badly needed capital into their cash-starved economies.

Clearly, the Biden administration will need to take action regarding ransomware, and since bitcoin has become ransomware attacker's Achilles heel, disrupting the flow of bitcoin could operate as a promising prosecutorial modus operandi.

With a range of historically proven statutory weaponry at his disposal, together with the AMLA's whistleblower incentives and other added firepower, Biden could mobilize an already active cadre of federal law enforcement and regulatory agencies to orchestrate a national access theory crackdown.

This kind of Biden ransomware blitzkrieg might not only stifle ransomware growth but could also asphyxiate bitcoin's most notorious other uses[25] such as terrorism, illicit drug, gun and child pornography sales, and so many other crimes.

For a newly elected president, not a bad day's work by any measure.

---

*John Reed Stark is president at John Reed Stark Consulting LLC and senior lecturing fellow at Duke University Law School. He previously served for almost 20 years in the SEC's Division of Enforcement Division, the last 11 of which as chief of its Office of Internet Enforcement.*



[1] Some cryptocurrency trading platforms go so far as to tout themselves as "a fully regulated and licensed cryptocurrency exchanges" and "regulated places to buy, sell and store Crypto." Yet in reality, despite their calling themselves "exchanges," no so-called crypto trading facility is one of the 27 exchanges actually registered with the SEC, and none are audited by the SEC exchange examination staff. (See complete list at https://www.sec.gov/fast-answers/divisionsmarketregmrexchangesshtml.html.)

[2] https://www.justice.gov/ag/page/file/1326061/download.

[3] https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[4] https://www.fincen.gov/msb-state-selector.

[5] https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering.

[6] https://www.law.cornell.edu/uscode/text/18/1960.

[7] https://www.justice.gov/archive/ll/highlights.htm.

[8] https://www.law.cornell.edu/wex/strict_liability.

[9] https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

[10] See, e.g. Press Release, "Russian National And Bitcoin Exchange Charged In 21-Count Indictment For Operating Alleged International Money Laundering Scheme And Allegedly Laundering Funds From Hack Of Mt. Gox," U.S. Dept. of Justice, U.S. Att'y's Office, N.D. Cal. (July 26, 2017), available at: https://www.justice.gov/usao- ndca/pr/russian-national-and-bitcoin-

exchange- charged-21-count-indictment-operating-alleged. See also, United States v. Murgio , 15-cr- 769(AJN), 2017 WL 365496 (S.D.N.Y. Jan. 20, 2017) and United States v. Faiella , 39 F. Supp. 3d 544 (S.D.N.Y. 2014). See also United States v. Budovsky , No. 13-cr-368 (DLC), 2015 WL 5602853, at *14 (S.D.N.Y. Sept. 23, 2015) (noting that 18 U.S.C. § 1960, which covers operation of an unlicensed money transmitting business, encompasses businesses that transmit virtual currency).

[11] https://www.sec.gov/spotlight/cybersecurity-enforcement-actions.

[12] https://www.sec.gov/news/press-release/2020-146.

[13] https://www.sec.gov/news/press-release/2020-262.

[14] https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading.

[15] https://www.jdsupra.com/legalnews/doj-and-irs-may-soon-begin-enforcement-51885/.

[16] https://www.journalofaccountancy.com/issues/2018/mar/irs-summons-of-coinbase-records.html.

[17] https://www.irs.gov/irm/part25/irm_25-005-007.

[18] https://www.irs.gov/pub/irs-pdf/f1040s1.pdf.

[19] William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, H.R. 6395. Division F of the NDAA is the Anti-Money Laundering Act of 2020, and Title XCVII within the bill contains additional provisions relevant to the financial services industry.

[20] AMLA, § 6314 (adding 31 U.S.C. § 5323(b)(1)).

[21] https://www.gibsondunn.com/the-top-10-takeaways-for-financial-institutions-from-the-anti-money-laundering-act-of-2020/#_ftn5.

[22] AMLA, § 6105.

[23] AMLA, §§ 6106, 6107, 6108.

[24] AMLA, §§ 6207, 6208, 6303.

[25] https://www.justice.gov/ag/page/file/1326061/download.