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

States' Crypto Enforcement Onslaught Has Only Just Begun

By **John Reed Stark** (June 1, 2018, 1:43 PM EDT)

John Reed Stark

Chalk it up to digital bravado. Wind Wide Coin, a cryptocurrency firm, brazenly used photos of none other than Jennifer Aniston and Prince Charles to provide glowing testimonials about their crypto products. Suffice is to say that neither the eminent prince nor the celebrated "Friend" had lent their likenesses to Wind Wide Coin's crypto campaign.

But not to worry. Thanks to the Texas State Securities Board, Wind Wide Coin has been shut down. The state of Texas has issued a cease-and-desist order against Wind Wide Coin and has also gallantly returned the hijacked identities of the eminent British royal and famed American icon back to their rightful owners, striking a blow for improved U.S.-U.K. relations.

While admittedly outrageous and almost laughable, the Wind Wide Coin case conveys far more than a message about the perils of identity theft and cryptocurrency fraud. Wind Wide Coin, and a slew of other prosecutions and enforcement actions brought by Texas and other U.S. states, have put crypto promotors on notice: Move over SEC, FinCEN, CFTC, IRS, FTC and the rest of the federal alphabet soup, because U.S. state regulatory and law enforcement authorities have begun a crypto enforcement rampage, with no end in sight.

Along those lines, on May 21, 2018, the North American Securities Administrators Association, or NASAA, announced, Operation Cryptosweep, one of the largest coordinated series of enforcement actions by state and provincial securities regulators in the United States and Canada to crack down on fraudulent initial coin offerings, cryptocurrency-related investment products and those behind them.

NASAA is the national voluntary membership association of the securities regulatory authorities in the 50 states, the District of Columbia, Puerto Rico, and the U.S. territories, as well as the provincial and territorial authorities in Canada and Mexico. NASAA members from more than 40 of its jurisdictions throughout North America participated in Operation Cryptosweep, comprised thus far of nearly 70 inquiries and investigations and 35 pending or completed enforcement actions related to ICOs or cryptocurrencies since the beginning of May 2018.

NASAA members are also conducting numerous other investigations into potentially fraudulent conduct that may result in even more enforcement actions. These actions are in addition to more than a dozen enforcement actions previously undertaken by NASAA members regarding these types of products. Many NASAA members are also conducting public outreach initiatives to warn investors in their jurisdictions of the risks associated with ICOs and cryptocurrencies.

Along these lines, Joseph Borg, NASAA president and director of the Alabama Securities Commission, stated fiercely:

> The persistently expanding exploitation of the crypto ecosystem by fraudsters is a significant threat to Main Street investors in the United States and Canada, and NASAA members are committed to combating this threat. Despite a series of public warnings from securities regulators at all levels of government, crypto-criminals need to know that state and provincial securities regulators are taking swift and effective action to protect investors

and provincial securities regulators are taking swift and effective action to protect investors from their schemes and scams.

These actions are clearly a follow-up to NASAA's Jan. 4, 2018, statement captioned "NASAA Reminds Investors to Approach Cryptocurrencies, Initial Coin Offerings and Other Cryptocurrency-Related Investment Products with Caution," which also highlighted the risks of cryptocurrency-related investments. Per the NASAA statement:

> Some common concerns investors should consider before investing in any offering containing cryptocurrency include:

- Cryptocurrency is subject to minimal regulatory oversight, susceptible to cybersecurity breaches or hacks, and there may be no recourse should the cryptocurrency disappear.
- Cryptocurrency accounts are not insured by the Federal Deposit Insurance Corporation (FDIC), which insures bank deposits up to $250,000.
- The high volatility of cryptocurrency investments makes them unsuitable for most investors, especially those investing for long-term goals or retirement.
- Investors in cryptocurrency are highly reliant upon unregulated companies, including some that may lack appropriate internal controls and may be more susceptible to fraud and theft than regulated financial institutions.
- Investors will have to rely upon the strength of their own computer security systems, as well as security systems provided by third parties, to protect purchased cryptocurrencies from theft.

State Jurisdiction

While the actual logistics of the jurisdiction of individual U.S. states regarding investing can vary, all states can assert jurisdiction over securities transactions and crypto-related subject matter. There exists no federal jurisdictional preemption.

Some state securities administrators are appointed by secretaries of state, some fall under the jurisdiction of their states' attorneys general, some are independent commissions, and others are appointed by their governors and cabinet officials. But whatever their title or structure, state securities administrators are often the first line of defense for Main Street investors.

In fact, securities administrators in each state are responsible for enforcing state securities laws, licensing firms and investment professionals, registering certain securities offerings, examining broker-dealers and investment advisers, and providing investor education programs and materials to their constituents.

How state securities administrators actually conduct their investigations and initiate their prosecutions remains a mishmash of 50 different and varying state regimes. Most state securities administrators have only civil authority and must refer their state criminal actions to an independent prosecutorial agency. Others, like the Texas Securities Board and the New York Attorney General's Office, are more powerful and have their own statutory jurisdiction over administrative, civil and even criminal actions to address securities violations.

With respect to crypto-related issues, some states are extraordinarily active while others are just beginning to join the fray. For instance, on March 27, 2018, the top securities regulator in Massachusetts issued consent orders halting five initial coin offerings — including projects that sought to raise capital to assist families affected with cancer and to support the programming for children — based on allegations that the token sales constituted unregistered securities offerings in violation of Massachusetts state law.

Texas has also become an active regulator of virtual currency activity. Between December 2017

and February 2018, the Texas State Securities Board issued five emergency cease-and-desist orders to respondents engaged in various forms of virtual currency activity, including issuing unregistered securities to Texas residents or to unaccredited investors and making misrepresentations related to cryptocurrency ventures.

More recently, on March 7, 2018, the New Jersey Bureau of Securities sent a cease-and-desist order to Bitcoiin (not to be confused with bitcoin), ordering the company to stop offering for sale any security in New Jersey until it is properly registered. Also, on Feb. 9, 2018, the New Jersey Bureau of Securities ordered bitcoin-related investment pool Bitstrade to stop offering its goods in New Jersey. According to the regulator, Bitstrade, which claims to take customers' bitcoin and invest the funds in the stock market, had been offering the equivalent of securities, but had not registered with the New Jersey government.

New York State

Not surprisingly, the New York Attorney General's Office, which has traditionally maintained an active and wide-ranging presence in the financial markets, has also stepped up its investigative efforts relating to cryptocurrency. And New York is focusing not just on ICOs but also on the rapid rise of crypto trading platforms, a very serious concern of the U.S. Securities and Exchange Commission (which issued, on March 7, 2018, its own broad and sweeping statement about the dangers of potential illegalities of exchange-like crypto trading facilities).

Specifically, the Investor Protection Bureau of the New York Office of the Attorney General launched its Virtual Markets Integrity Initiative, a fact-finding inquiry into the policies and practices of platforms used by consumers to trade virtual or cryptocurrencies like bitcoin and ether. As part of a broader effort to protect cryptocurrency investors and consumers, the New York Attorney General's Office sent questionnaires to 13 major virtual currency trading platforms requesting key information on their operations, internal controls and safeguards to protect customer assets. As the letters explain, the initiative seeks to increase transparency and accountability as it relates to the platforms retail investors rely on to trade virtual currency, and better inform enforcement agencies, investors and consumers.

The New York attorney general cites "reports of the theft of vast sums of virtual currency from customer accounts, sudden and poorly explained trading outages, possible market manipulation, and difficulties when withdrawing funds from accounts." Thus, trading platforms are also requested to describe their anti-money laundering programs, their know-your-customer practices, the fiat and virtual currencies that they trade, and locations where they do and do not accept customers.

The New York attorney general sent letters to the following virtual currency trading platforms and may send out a second wave for others at a later date: (1) Coinbase Inc. (GDAX), (2) Gemini Trust Co., (3) BitFlyer USA Inc., (4) iFinex Inc. (Bitfinex), (5) Bitstamp USA Inc., (6) Payward Inc. (Kraken), (7) Bittrex Inc., (8) Circle Internet Financial Ltd. (Poloniex LLC), (9) Binance Ltd., (10) Elite Way Developments LLP (Tidex.com), (11) Gate Technology Incorporated (Gate.io), (12) itBit Trust Co., and (13) Huobi Global Ltd. (Huobi.Pro).

The initiative was the first public venture into the cryptocurrency regulatory territory, which was already occupied since 2015 by another New York state agency, the New York State Department of Financial Services, or DFS. Back then, the DFS instituted its BitLicense Framework, which requires companies engaged in certain virtual currency business activities involving New York or its residents to complete a detailed license application and maintain ongoing compliance with a comprehensive set of rules relating to cybersecurity policies, procedures, consumer protections, asset safeguarding, anti-money laundering, regulatory exams and reporting requirements.

Ironically, the 13 recipients were not limited to those trading platforms that hold a license to operate as a virtual currency business in the state of New York (there are currently only four such virtual currency business activity license, or "BitLicense" holders). In fact, the attorney general's requests explicitly acknowledge that certain of the recipients may have opted not to offer services in New York in order to avoid the state's licensing requirements.

Not all of the 13 named trading platforms reacted positively to the inquiry. Kraken slammed the inquiry, refused to participate and demanded regulators refrain from "handing down

inquiry, refused to participate and demanded regulators refrain from "handing down commandments from the ivory tower." In "Kraken's Position on Regulation," Kraken states boldly (and somewhat obnoxiously):

> To be fair, we would have given the same response to the AG of North Korea. We would be happy to work with the NYAG and the NYDFS (again) on a strategy for replacing the BitLicense with something rational. However, that engagement would be voluntary, not on any arbitrary deadline and we would expect NY to be respectful of our time, to do its own research and come to the discussion prepared. We would do this for free, as a gift to the people of New York.

In stark contrast, other exchanges have (at least publicly) embraced the attorney general's inquiry. Gemini's CEO, Tyler Winklevoss, noted,

> Gemini applauds the Attorney General's focus on this industry and the Virtual Markets Initiative, and we look forward to cooperating with and submitting our responses to the questionnaire that has been circulated.

In a blurred and somewhat lukewarm reaction, Bitrex released a statement espousing neither the embracing of, nor an anger with, the initiative:

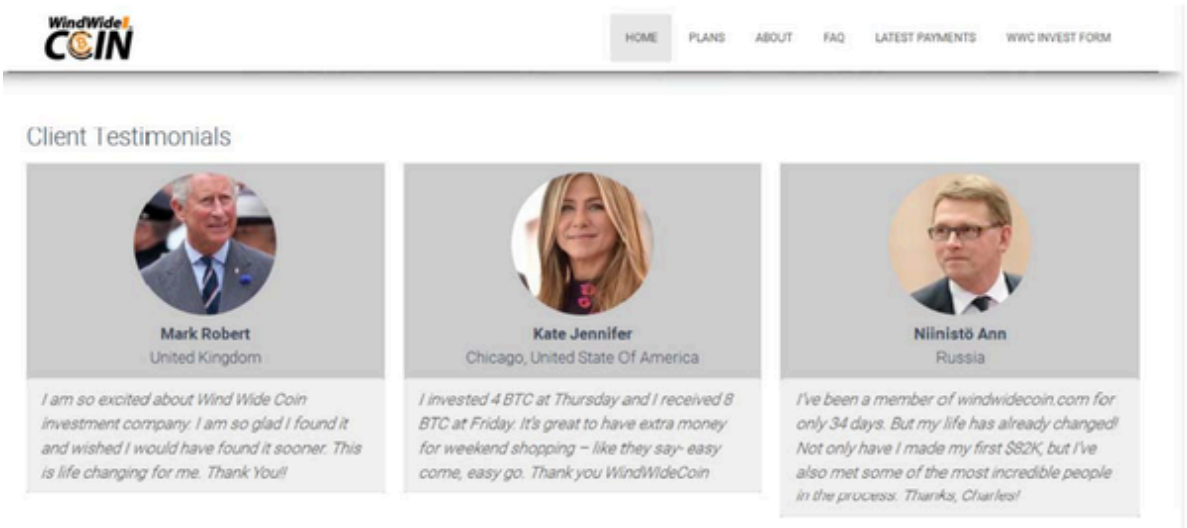
> Bittrex supports building a secure, fully-compliant environment for blockchain that encourages innovation, economic growth, and U.S. leadership in the industry, and that is why we are proactively engaged in discussions with regulators regarding how this may be accomplished with thoughtful policymaking. We look forward to working with [now former] NY Attorney General [Eric] Schneiderman on our shared goal of improving transparency, accountability and security across all virtual currency trading platforms.

Under any circumstance, New York's initiative will likely serve as the opening salvo against these crypto trading platforms, and could lead to fines, penalties and even jail time for the firms and perpetrators of any securities violations that New York discovers. Moreover, the initiative is likely the beginning of a comprehensive examination of cryptocurrency markets by not just New York, but plenty of other state regulatory authorities as well.

Digital Bravado

The cases brought by the various state securities administrators in Operation Cryptosweep vary considerably but demonstrate both the outrageous nature of certain crypto-related frauds and the threat to Main Street investors that these schemes represent. Some of the digital evidence from a few of the Texas State Securities Board's enforcement actions of Operation Cryptosweep is particularly compelling — not just in its boldness but also its sheer bravado. Below is a quick look at three of Texas' enforcement actions, including Wind Wide Coin.

Wind Wide Coin



Texas Securities Commissioner Travis J. Iles entered an emergency cease-and-desist order on May 15 to stop Wind Wide Coin Inc., an entity that says it is based in Houston, from fraudulently offering investments in a cryptocurrency trading program.

The order alleges that Wind Wide Coin and three sales agents in Houston were offering for sale investments in a cryptocurrency trading program that uses an "automatic trading bot." The company allegedly promised investors the combination of "no risk" and extraordinarily high returns. The purchase of 0.10 of bitcoin, for example, would return one bitcoin 24 hours later, a one-day return of 900 percent.

Wind Wide Coin's marketing allegedly extended to a rotating sequence of celebrity and political endorsements. The company's website allegedly featured a photograph of Jennifer Aniston, but identified her as "Kate Jennifer," an investor. Similarly, a photograph of Prince Charles was identified as "Mark Robert," another investor who provided a testimonial. The testimonial was then attributed verbatim to a "Johnson Smith," supposedly a U.K. investor. Finally, in an apparent effort to provide additional international appeal, Wind Wide Coin also allegedly used a photo of former Finland Prime Minister Matti Vanhanen for a third testimonial, identifying him as Nininstito Ann, from Russia.

Wind Wide Coin purportedly represents that its Houston office is in an office building at 5015 Mitchelldale, 77082 — yet, there is no building of any kind at that location. According to the order, Wind Wide Coin misled potential investors by claiming it is a "licensed company" and "legally registered." Neither the company nor the sales agents named in the order are registered to sell securities in Texas. Wind Wide Coin allegedly not only touted the success of its trading bot, but also boasted that returns paid to investors were tied to the principal deposit, not the success in trading cryptocurrencies.

Wind Wide Coin allegedly offered different levels of investment, starting with "baby" and moving up to "standard," "premium," "X-boost" and "ultimate." The "X-boost" plan, according to information on the company's website, required a minimum investment of one bitcoin and returns four bitcoins to the investor in four days. The price of one bitcoin was $8,688.47 at the close of trading May 14.

Wind Wide Coin allegedly provided no material information about how its trading bot operated or the background of its principals and trading professionals. Nor did Wind Wide Coin disclose to investors the numerous regulatory and market risks in bitcoin and other cryptocurrencies investing.

LeadInvest

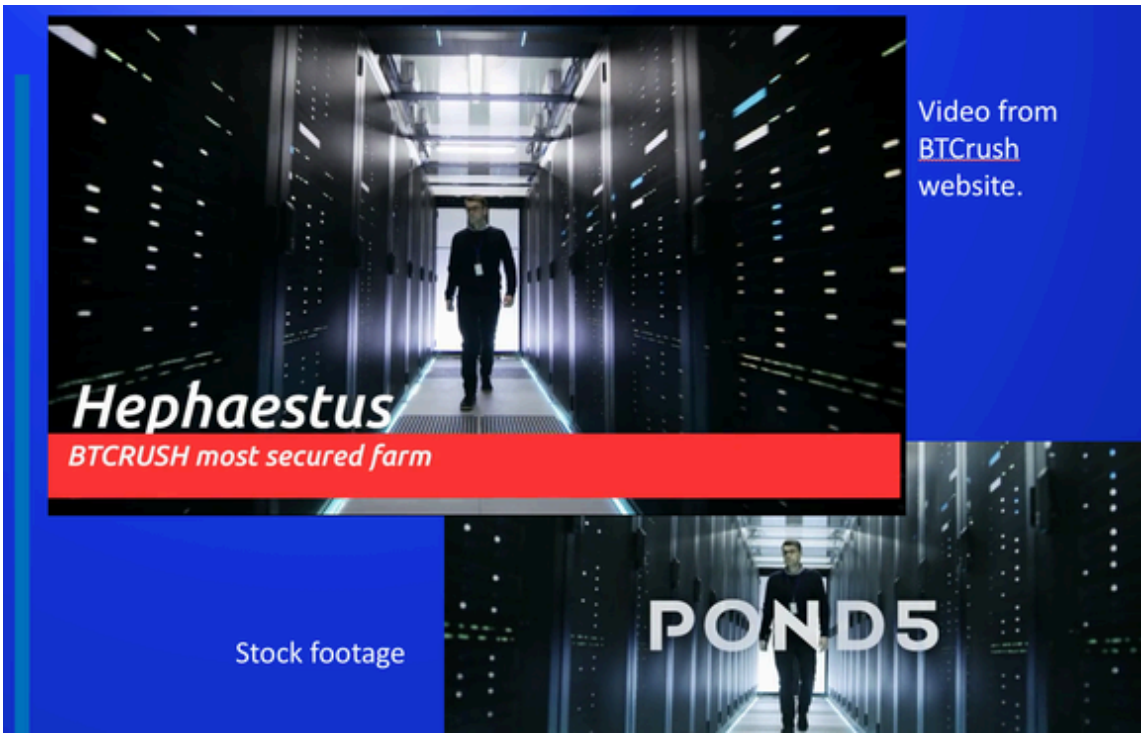
The Texas Securities commissioner also brought an emergency action against cryptocurrency firm LeadInvest, an offshore entity that claims it is advised by U.S. Supreme Court Justice Ruth Bader Ginsburg and three former U.S. solicitors general. Specifically, on Feb. 26, 2018, Texas Securities Commissioner Travis J. Iles entered an emergency cease-and-desist order against LeadInvest to stop its fraudulent offers of various investments, including one tied to a cryptocurrency mining program in Iceland.

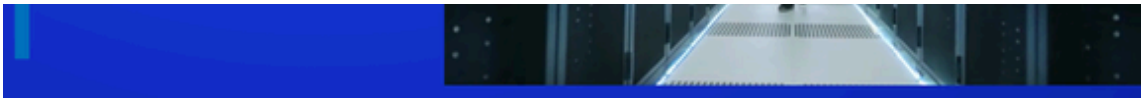
LeadInvest was allegedly using public advertisements to lure Texans to its website, which contained profiles and photographs that purported to depict its team, advisers and legal professionals.

An alleged photograph of LeadInvest's legal professionals portrayed Justice Ginsburg and former Solicitors General Theodore Olson, Paul Clement and Seth Waxman. The photograph was first printed in the fall 2005 edition of the GW Law Briefs, a publication of the George Washington University Law School. The order alleges that LeadInvest was deceiving the public through its use of the photograph to tout its legitimacy.

Texas' Securities Enforcement Division also determined that other images used by LeadInvest were merely stock photographs of models sold on the internet. Other photographs were actually images from unrelated websites that depict an attorney licensed to practice in Texas, an attorney licensed to practice in North Carolina, and a law firm based in California.

BTCrush





On May 8, 2018, Texas Securities Commissioner Travis J. Iles entered two emergency actions against unregistered promoters for fraudulently offering high-return investments in programs tied to cryptocurrencies.

According to the orders, Bitcoin Trading & Cloud Mining Ltd. also known as BTCrush, and Forex EA & Bitcoin Investment LLC were violating the Texas Securities Act by failing to disclose any material information about their principals, strategies, finances, and the extensive technical and regulatory risks of cryptocurrency-related offerings.

BTCrush, whose principals list an address in London, was allegedly soliciting Texas investors with the promise of huge returns from the mining of cryptocurrencies at three massive computing centers featured in videos on the company's website.

The videos were not evidence of anything, however. According to the order, BTCrush created the videos by manipulating stock footage available for sale on the internet. BTCrush allegedly doesn't disclose the locations of the sites but described one as "a secluded place in the mountains hiding incredible computing power." Another site was purportedly located in a bombproof shelter from "the Second World War times."

BTCrush allegedly described itself as a cloud-based cryptocurrency mining company that mines both bitcoin and other virtual currencies, known as alt-coins. The company allegedly offered investments in a program to sell newly created alt-coins to buy bitcoins.

BTCrush purportedly claimed that an investment in its mining investment program had been paying 4.1 percent interest daily on a lifetime contract since going live on March 8, 2018. According to the order, that meant a $10,000 investment would return $410 per day and $149,650 over one year.

BTCrush allegedly promised investors a "100% satisfaction guarantee," but also "reserved the right to amend" the interest rate it pays "without agreement from investors." The company allegedly promised investors that a $5,000 investment would return $50,000 in 21 days, while intentionally failing to disclose its trading strategy and the widespread risk in trading bitcoin and foreign currencies.

Looking Ahead

The SEC has already made it clear that it intends to crack down on cryptocurrency financiers who violate U.S. securities laws and threaten injury to investors. Now the states, in an effort to protect investors in their respective jurisdictions, are clearly stepping up and following suit. Just recently, it was reported that the U.S. Department of Justice has launched a criminal probe into cryptocurrency price manipulation — no doubt NASAA and its many state securities administrator members will be participating in this effort as well.

What strikes me most about Operation Cryptosweep is the extraordinary swiftness of the myriad investigations and prosecutions. There has rarely been such a rapid-fire operation in the history of securities regulation and enforcement.

It was only a few months ago that Operation Cryptosweep actually began, when NASAA organized a task force of its member state and provincial securities regulators to begin a coordinated series of investigations into ICOs and cryptocurrency-related investment products. Regulators identified many cryptocurrency-related products and, as part of its efforts, the task force identified hundreds of ICOs in the final stages of preparation before being launched to the public. These pending ICOs were advertised and listed on ICO aggregation sites to attract investor interest. Many have been examined and some were determined to warrant further investigation.

Meanwhile, NASAA President Joseph Borg has signaled that more crypto-related enforcement actions are in the works, stating in the Operation Cryptosweep press release, "The actions announced today are just the tip of the iceberg," noting that the task force also found

announced today are just the tip of the iceberg," noting that the task force also found approximately 30,000 crypto-related domain name registrations, the vast majority of which appeared in 2017 and 2018.

Of course, with respect to the broad range of violations of ICOs and cryptocurrency trading platforms, some securities lawyers like myself view these prosecution akin to shooting fish in a barrel, because the violations are so apparent and clear-cut. But there is even more to this notion.

Any former SEC enforcement lawyer will attest that crypto-related cases are typically not difficult, cumbersome or costly to investigate — and do not require much in terms of resources. Here's why: Cryptocurrency-related investigations are not like accounting frauds, market manipulations or complex insider trading cases, requiring extensive review of financial statements, audit trails and/or market data. Nor do crypto-related investigations typically require the conducting of intense financial or digital forensics, lengthy document reviews, and/or multiple testimonial proceedings. Instead, crypto-related investigations actually require scant evidence gathering.

In fact, the internet provides SEC staff a glimpse into cryptocurrency exchange operations and ICO promotions as they unfold without ever using a subpoena. This has proven to be the most profound change wrought by the internet in the field of securities regulation. Far from tying regulators' hands, the internet has become the virtual rope that many cyberthieves use to hang themselves.

Moreover, unlike hackers trying to tamper with the energy grid or clandestinely trying to intrude into the computer networks of public companies, cryptocurrency financiers want to be found. They require a wide audience to review their information, invest in their offering, or participate in their exchange. Rather than hide amid the unseen underbelly of the internet, ICO promoters and cryptocurrency exchange operators peddle their services in plain view 24-7, and can be actively observed from virtually anywhere on the planet.

Relatedly, outside of fraud claims, most SEC crypto-related violations are strict liability, requiring little in the way of scienter, conspiracy or even motive. As a matter of law, every securities offering is either registered, exempt or unlawful — regardless of what anyone in the process honestly believes or testifies.

So it should come as no surprise that state securities administrators have boosted their own crypto enforcement efforts. Because while crypto promoters can find easy prey in today's excitable (and sadly gullible) retail investor marketplace, ICOs and crypto trading platforms are also easy to surveil, easy to identify, and easy to charge.

John Reed Stark is the president of John Reed Stark Consulting LLC, a data breach response and digital compliance firm. Formerly, Stark served for almost 20 years in the Enforcement Division of the U.S. Securities and Exchange Commission, including 11 years as the chief of its Office of Internet Enforcement. He is the author of "The Cybersecurity Due Diligence Handbook."

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

All Content © 2003-2018, Portfolio Media, Inc.