View as Webpage

Issue 8, 2020

Attorney General William P. Barr Announces Publication of Cryptocurrency Enforcement Framework

"The Framework provides a comprehensive overview of the emerging threats and enforcement challenges associated with the increasing prevalence and use of cryptocurrency; details the important relationships that the Department of Justice has built with regulatory and enforcement partners both within the United States government and around the world; and outlines the Department's response strategies."

Why this is important: The Office of the Attorney General has published guidance regarding cryptocurrency and the regulation and enforcement surrounding the technology. The publication has an expansive scope and includes an overview discussion of common uses of cryptocurrency – both legitimate and illicit – as well as the laws and regulations dealing with cryptocurrency. It also discusses business models that may facilitate criminal activity with cryptocurrency. This publication represents a major step toward an overarching regulatory framework that would apply to all cryptocurrency in the U.S. It also essentially serves to cement the acceptance of cryptocurrency within the economic system of the U.S. and internationally. The Department of Justice certainly will tailor its policies and procedures regarding cryptocurrency in order to find the most efficient balance between freedom of use and regulation of the technology. As with many revolutionary technologies, the DOJ won't get it right the first time, but this publication indicates continued progress toward the best economic benefit. Stay tuned to future issues of *Decoded* as we'll take a deeper dive into this publication and other issues related to cryptocurrencies in our next video companion. --- P. Corey Bonasso

---

IBM Executive Says Blockchain Becoming a Useful 'Real Business Tool'

"IBM Blockchain's general manager explains the changing role of blockchain and how it will be applied to IBM's hybrid cloud solution."

Why this is important: This is an interesting interview with IBM Blockchain's general manager discussing the evolution of blockchain technology from a novel technology to an important business tool and some of the use scenarios IBM is developing and what the manager sees in other industries. As the manager put it, business conversations about the use of blockchain in industries are "mainstreaming" to a point where the word "blockchain" isn't even mentioned. The manager summed it up well when saying blockchain is being implemented to address industries' concerns about "provenance, track and trace, and dispute resolution." --- Nicholas P. Mooney II

Venezuela Rolls Out Ethereum-Based Stock Exchange to Help Skirt U.S. Sanctions

"A draft of a wider 'Anti-blockade Law for National Development and the Guarantee of Human Rights,' aimed to give the government tools to 'defeat all mechanisms of persecution and international blockade,'

was also announced."

Why this is important: Venezuela: oil producer and...fintech leader? The latter might soon come true as a result of new Venezuelan legislation that uses the blockchain as a backend for the trading of stocks, bonds, and real estate in an effort to avoid strict U.S. sanctions. This development is certain to draw the attention of both U.S. and international politicians concerned about the use of fintech platforms by so-called "bad actors," but it also is a fascinating circumstance-driven laboratory for innovation. If Venezuela's decentralized national exchange is successful, for instance, it could drive government and private industry to follow. For these reasons, Venezuela's experience merits close attention. --- Joseph V. Schaeffer

---

Paying Ransomware Demands Could Land You in Hot Water with the Feds

"Advisory applies not just to victims but also to security and finance firms they hire."

Why this is important: Companies who fall victim to ransomware attacks now have another worry to deal with – the federal government. The U.S. Department of Treasury published guidance in an advisory last week that warned that ransom payments made to certain entities or entities in certain countries with a "sanction nexus" could lead to penalties by the Office of Foreign Assets Control ("OFAC"). Most companies are anxious to pay demands from ransomware attacks because the amount of data they stand to lose could cripple them. Furthermore, OFAC also could levy penalties against third parties that assist with facilitating ransomware payments, such as financial institutions. The government's reasoning behind this guidance is that it rewards the criminal behavior with no guaranty that the company's data will be returned. Once a hacker has obtained a company's data, it could copy it and use it for further malicious actions, even after receiving a ransom payment. The company also likely would not have a way of knowing if its information is being used by hackers in such a way. Companies have been learning to navigate ransomware attacks and other various data breaches continuously for many years, and this creates another factor for companies to consider when fashioning their data security protocols. --- P. Corey Bonasso

---

Ransomware Hits Healthcare Provider UHS, Shuts Down Hospital IT Systems

"Although Universal Health Services largely runs behavioral healthcare facilities, it also operates some emergency care centers, potentially putting patients' lives at risk."

Why this is important: We devote a lot of attention to data security and cybersecurity in *Decoded*, and for good reason: a successful data breach or cyberattack can lead to millions of dollars in damages, not to speak of the reputational harm. And though no business sector is immune, few have more risk than the healthcare sector. A recent report claims that Universal Health Services ("UHS"), a company operating 400 hospitals and behavioral facilities in the U.S. and the UK, has been hit by a ransomware attack that has shut down all computer access and required UHS to turn patients away. The company, for its part, acknowledges technological interruptions while placing blame on an IT security issue. But regardless of cause, the potential for a breach of this kind—and one that potentially impacts patient care—should put the healthcare sector on notice that a full data security and cybersecurity audit is well past due. --- Joseph V. Schaeffer

---

ACLU Opposition to the Use of Remote Proctoring for the California Bar Examination

"'As the Exam date approaches, we remain wary of the State Bar's plans to utilize remote proctoring technology due to the discriminatory impact this decision has had, and will continue to have, on test takers from marginalized groups.'"

Why this is important: Each July, thousands of prospective lawyers gather across the country to sit for an in-person bar exam—the legal profession's licensing exam. Because of the COVID-19 pandemic, however, several states have not only moved their exams to the fall, they've moved them online, too. This latter move online has prompted new approaches to proctoring, with the leading provider of testing software, ExamSoft, adopting facial recognition technology to verify test-takers' identities and ensure that they remain present during the test. The ACLU Foundations covering California, however, argued to

that state's Supreme Court that the use of facial recognition technology raises significant racial justice and privacy and security concerns. In addition to studies finding that facial recognition technology struggles to identify and distinguish people of color, an Arab-American applicant and Black applicant reported that the ExamSoft software could not confirm their identities—or could only do so under unusually bright light. Moreover, the ACLU Foundations raised the prospect that this facial recognition data, along with other personal data collected during the exam process, could present an alluring target for cyber criminals. For now, these concerns seem to have made little headway, with several states having completed their online bar exams. But these same issues are likely to recur in other contexts—and may be argued or even decided by lawyers whose experiences have been shaped by the bar exam debate. --- Joseph V. Schaeffer

---

Owners of BitMEX, a Leading Bitcoin Exchange, Face Criminal Charges

"American authorities brought criminal charges against the owners of one of the world's biggest cryptocurrency trading exchanges, BitMEX, accusing them of allowing the Hong Kong-based company to launder money and engage in other illegal transactions."

Why this is important: Coconuts are for eating, not for bribes. The owners of one of the world's largest cryptocurrency exchanges has learned this recently. The "Bitcoin Mercantile Exchange," or BitMEX, was incorporated in the Seychelles and maintained offices in New York and Hong Kong. Federal authorities had been investigating BitMEX for its refusal to put in place anti-money laundering controls, among other things, and alerted the owners of BitMEX to the authorities' concerns. Its CEO is said to have responded that he incorporated BitMEX in the Seychelles because it costs less to bribe Seychellois authorities -- just a coconut -- than it would cost to bribe authorities in the U.S. Although BitMEX maintained that it cut ties with all customers in the U.S., thereby depriving it of any jurisdiction, the government's position is BitMEX maintained offices in New York and willfully included U.S. citizens as customers. The real importance here, and the subsequent arrests of BitMEX's owners, is to show that the cryptocurrency exchanges and trading are not the wild west some people believe, and the U.S. government will take seriously the requirement that exchanges implement "Know Your Customer" and anti-money laundering controls. --- Nicholas P. Mooney II

Why Every U.S. Congressman Just Got Sent Some 'American' Bitcoin

"As well as lining their virtual wallets, the blockchain advocacy group hopes the program will educate Congress about blockchain."

Why this is important: There are many unanswered regulatory questions surrounding cryptocurrency, but the Digital Chamber of Commerce Political Action Committee has developed an idea that may get some answers. The PAC, in a program it is calling "Crypto for Congress," is donating $50 in American Bitcoin to every member of Congress and sending an online educational toolkit in an effort to educate lawmakers about cryptocurrency. By educating Congress, the PAC is hoping to get some "regulatory clarity around cryptocurrencies, notably ICOs, as well as tax guidance and anti-money laundering measures." When a company attempts an initial coin offering, it is often uncertain under which regulatory regime their particular cryptocurrency will fit. For example, if their cryptocurrency fits the definition of an investment contract, it falls within the purview of the SEC. However, what constitutes an investment contract is far from a bright-line rule. Additionally, the PAC is hopeful that Congress will use what it has learned about cryptocurrency to "draft a plan on how to become the world leader in blockchain." Perhaps giving Congress a personal stake and an education in cryptocurrency will finally incentivize them to develop a regulatory regime for cryptocurrency, thus making things clearer and expanding the nation's presence in the cryptocurrency space. --- Kellen M. Shearin

---

House Judiciary Committee Releases 449 Page Report on 'Investigation of Competition in Digital Markets'

"As expected, the investigation found that today's big tech companies (Amazon, Apple, Facebook, and Google) have become monopolies."

Why this is important: The 449-page "Investigation of Competition in Digital Markets" report has been issued regarding the House of Representatives' investigation into "Big Tech." The report claims that the

big four -- Amazon, Apple, Facebook, and Alphabet (Google) -- take steps to stifle competition, including acquiring companies and selling products below costs, all to eliminate rivals. One Congressman advised the report is a "thinly veiled call to break up" the big four companies, a move with which he doesn't agree. Nonetheless, there are provisions in the report with which even its detractors agree. One of the report's recommendations calls for a lowering of the burden of proof for the Justice Department and Federal Trade Commission to stop company mergers. Another addresses steps to allow consumers to take greater control over their personal data, including fostering "data portability and interoperability between platforms." --- Nicholas P. Mooney II

Anthem to Pay $39M to State AGs to Settle Landmark 2015 Data Breach

"In 2015, Anthem was hit with a massive cybersecurity breach that put about 80 million individuals' data at risk, including current and former customers, current employees and even Anthem's CEO, Joseph Swedish."

Why this is important: The Anthem data breach offers three lessons on the importance of prevention and risk mitigation. First, the threat is real and sophisticated: the person behind the Anthem data breach is believed to be a Chinese national who worked with a larger hacking group. Second, the fallout from a data breach is long-lasting, with Anthem settling legal issues a full five years after the breach occurred. And third, the consequences are significant. In addition to the $39.5 million settlement with State Attorneys General, Anthem will have paid an additional $16 million to the Department of Health and Human Services and $115 million to affected individuals. --- Joseph V. Schaeffer

---

Airlines Launch Trial of an App that Would Verify Travelers' Coronavirus Test Results

"Called CommonPass, the app is being rolled out this month for some passengers flying to or from London, New York, Hong Kong and Singapore on Cathay Pacific Airways and United Airlines."

Why this is important: There is one tool that is being tested to make the post-COVID "new normal" a little easier. The "CommonPass" app is being tested on United Airlines and Cathay Pacific Airways flights to and from London, New York, Hong Kong, and Singapore. The app contemplates that a passenger will take a COVID-19 test prior to arriving at the airport. The test results are certified by a laboratory and uploaded into CommonPass, which also may house the passenger's vaccination records. The app creates a QR code that the passenger presents to airline officials, ensuring that the passenger is safe to enter the new city or country. The purpose of the app is to reduce wait times at airlines and blanket quarantines in some countries. --- Nicholas P. Mooney II

Operating Rooms Turn to Zoom-Like Technology for the Age of Covid

"A $100 million funding round for startup Avail promises to bring social distancing to surgical operations."

Why this is important: The COVID-19 pandemic has disrupted several industries and economic sectors since the early part of 2020, but silver linings are still being realized. A startup based in Palo Alto, California is increasing its production of "telemedicine consoles," which are devices that allow surgeons performing live procedures to collaborate with long-distance viewers following via a tablet or laptop. Rather than a crowded operating room full of students and doctors all straining to get a look at the surgeon's technique, this technology allows presumably unlimited viewers to get an up close and personal look at every cut of the surgeon's scalpel. The consoles feature a high powered camera with the capability of projecting images up to 30 times their actual size. This sort of direct access to the best surgeons in the world could greatly accelerate the learning curve for new surgeons practicing new techniques. This technology also could affect malpractice suits against doctors because many surgeries now can be filmed. Furthermore, new surgeons who are learning the safest and most innovative techniques more quickly also could lead to higher quality surgeons across the board and fewer malpractice cases in general. --- P. Corey Bonasso

---