SHARE:

Join Our Email List

View as Webpage

March 2, 2022

Welcome

Welcome to our fourth *Decoded* issue of the year!

Like the rest of the world, we have been watching as events unfold in Ukraine. This issue covers one of the lesser known aspects in that conflict, that is, the extent to which cryptocurrency may impact what is being called "the world's first crypto war."

We also cover interesting news in other fields such as healthcare data breaches; future of health information technology; the IRS, crypto and NFTs; CRISPR patents; risks with biometric id systems; board liability and cybersecurity; vaccine passports; cross-border payments; and mRNA and medical treatment breakthroughs.

We hope you enjoy this issue and, as always, thank you for reading.

Nicholas P. Mooney II, Co-Editor of *Decoded* and Chair of Spilman's Technology Practice Group

and

Alexander L. Turner, Co-Editor of *Decoded*

War in the Time of Crypto

"In the Russia-Ukraine conflict, which side is crypto helping? Both."

Why this is important: The world continues to watch Russia's invasion of Ukraine as it dominates news outlets. An angle that might not be realized is the impact cryptocurrency may have. Before the invasion, Ukraine was a top European adopter of cryptocurrency and ranked as the fourth biggest in the world. In September 2021, it legalized its use. At the same time, Russia has emerged as a leader of illicit cryptocurrency activity, including ransomware attacks and cryptocurrency-based money laundering. Since the invasion started, there have been hundreds of thousands of dollars in cryptocurrency donations

raised to support the Ukrainian army. Western cryptocurrency activists are calling on people to mobilize and raise more to support the Ukrainian people. One cryptocurrency exchange gave $25 to each Ukrainian on its exchange. There also are fears that Russia could turn to cryptocurrency as a means to avoid Western sanctions, though some commentators believe that fear is unlikely to materialize due to the lack of infrastructure to integrate cryptocurrency into Russia's financial system. The extent to which cryptocurrency will actually influence this conflict remains to be seen, but this issue is an important one to watch as the conflict continues. --- Nicholas P. Mooney II

CaptureRx to Consider Filing for Bankruptcy if $4.75M Settlement Not Approved

"The incident was one of the largest healthcare data breaches of 2021."

Why this is important: One cyberattack can bankrupt your company if you do not have sufficient insurance coverage. CaptureRx assists hospitals with their 340B drug programs, which provide patients with lower cost prescription drugs. A ransomware attack on CaptureRx in 2021 impacted 1.2 million patients whose protected health information was breached. As a result of the breach, 10 separate lawsuits were filed. In an attempt to resolve these suits, CaptureRx proposed a $4.75 million settlement, which would entitle each class member to a $25 payment, and each California subclass member to a $100 payment. Additionally, CaptureRx's customers, like MetroHealth System and Walmart, are seeking indemnity from CaptureRx for the disclosure of their patients' and customers' protected health information. The CaptureRx matter demonstrates why it is so important to obtain sufficient insurance coverage for cyberattacks. CaptureRx's insurance policy is a wasting policy that erodes as the case progresses and attorneys' fees and settlements are paid. As a result, the $4.75 million settlement is only half funded by insurance, and the other half is out of the CaptureRx owners' pockets. As a result, if this settlement offer is not accepted, CaptureRx says that it will likely have to file for bankruptcy. Avoiding situations like the one CaptureRx now finds itself in is why pre-emptive cybersecurity and adequate insurance coverage is so critical. --- Alexander L. Turner

---

Delivering on the Promise of Health Information Technology in 2022

"This year providers, patients, payers, public health practitioners, technology developers, researchers, and other stakeholders will take the decade-long investment in health information technology to the next level."

Why this is important: The HITECH Act was signed into law in 2009, but the requirements for medical providers to maintain electronic health records were not fully operational until 2011. Many people thought that was the end of it. This year, another milestone for that process should occur, with true sharing of that electronic data nationwide. Technical infrastructure and policy developed nationwide may enable that. That's good! The article does not address the fact that this nationwide sharing, across different systems and software and borders, also may permit broader and more pernicious breaches. We'll see. --- Hugh B. Wellons

---

How the IRS is Looking for Its Share of Cryptocurrency and NFT Growth

"Tax professionals are not only battling the murky guidance issued by the Internal Revenue Service in this space but also struggle to understand what all the terminology means when dealing with digital assets."

Why this is important: A recurring issue in the cryptocurrency space in the U.S. is the regulation that already has been adopted, the inconsistency among regulations, when more regulation will be issued, and what it will look like. This article provides a good introduction to some of the tax issues involved in cryptocurrencies and non-fungible tokens ("NFTs") and comes at a great time with tax season upon us. It starts with IRS Notice 2014-21, where the IRS first weighed in on cryptocurrencies and stated that, for federal tax purposes, they will be treated as property. It provides an easy-to-understand discussion of

cryptocurrencies and NFTS as well as the tax issues inherent with trading them. Whether you're a tax professional, an active crypto and NFT trader, or someone who's interested in the issues in the space, this article is a good place to start to understand these issues. --- Nicholas P. Mooney II

Third-Party Vendor Morley Reports Data Theft Impacting 521K Individuals

"The incident is the second-largest healthcare data breach reported in 2022, so far."

Why this is important: Medical providers, a frequent target of cyberattacks, aren't the only entities who need to answer for insufficient protections of personal medical information. Less flashy, but still vulnerable are the third-party vendors used by medical providers for a range of services including data processing, storage, billing, and more. While patients may never have heard of these entities, they are critical links in the "supply chain" of medical information, and as seen here, breaches of third-party vendors can be even more catastrophic than that of medical providers, as vendors often hold data from numerous providers. Medical providers aren't off the hook for these third-party breaches either. Providers who own the data are responsible for ensuring that third-party entities are complying with HIPAA requirements as well. Providers must ensure proper contracting requirements are in place and must do their due diligence on providers before handing over their data. Providers may also be obligated to pay some or all of the costs associated with third-party breaches' investigations, notifications, and remediations, depending on the contract language. With so much liability and risk going around, entities will find their best protection in robust compliance programs. --- Risa S. Katz-Albert

---

New CRISPR Patent Hearing Continues High-Stakes Legal Battle

"Lawyers trade pointed exchanges over invention of genome editor."

Why this is important: We've written previously about CRISPR-Cas9 and its ability to allow editing of DNA. This article describes the battle over both who owns CRISPR and, as a result, who owns the results of using CRISPR to produce new products. Arguments about who owns intellectual property happen all the time. This instance is particularly important, because many labs use CRISPR to create new products. In order to do that, they must license the IP from the owners of CRISPR. Some have licensed from one, some from another. But, those who licensed from the "wrong" party may not really have a license! This may slow and even kill the development of many promising treatments. This even affects universities doing basic research. --- Hugh B. Wellons

---

Inside Look at an Ugly Alleged Insider Data Breach Dispute

"Consolidated Texas Court case alleges trade secret theft, fraud and intimidation."

Why this is important: Data breaches are not just the result of bad actors from outside your organization. They can also come from within, as is the case with Premier Management Co., which is an accountable care organization. Premier suffered two data breaches that resulted in the exposure of thousands of individual's protected health information. The data breach was caused by a former company officer, Mohammad Sohail, who then left to work for Premier's outside IT administrator, Wiseman Innovations, which Sohail also owned. After his departure from Premier, Sohail allegedly used his position at Wiseman to access Premier's confidential files and trade secrets. This intrusion into Premier's computer system also exposed the protected health information of thousands of individuals. The intrusion was accomplished by Sohail using his Premier "official issued laptop" that he did not return when he left Premier. Sohail was still able to access Premier's system with this laptop because he convinced Premier's IT administrator, who was also employed by Wiseman as an IT infrastructure and HIPAA officer, to change Premier's security controls. This included disabling the endpoint security and giving Sohail access to Premier's system even after he resigned from Premier. While it is difficult to protect against breaches caused by its own IT administrator, some simple acts could have prevented this data breach. The first is that upon departure, Premier should have required Sohail to turn over all company computers, laptops, tablets, cell phones, and other devices. The dual roles at Premier and Wiseman should have also raised red flags regarding issues around data access controls. A "wall" could

have been put up around Sohail's ability to access Premier's data, giving him only role-based access instead of complete or total access. Finally, Premier should have had a third-party auditor address these data access issues as part of an annual HIPAA risk analysis. These simple actions by Premier would have prevented Sohail's insider data breach and exposure of protected health information. --- Alexander L. Turner

---

The Enduring Risks Posed by Biometric Identification Systems

"But in doing so, these systems create risks for the people whose data is collected, ranging from how the data is stored to what happens if the collecting agency is not in ultimate possession of the data."

Why this is important: The best laid plans don't always pan out as anticipated. In this prime example, U.S Military technology using biometric data to ensure reliable identification verification, having fallen into Taliban hands poses an extreme risk for many. While this example is extreme, it begs the policy question of whether biometric data should be maintained at all and what safeguards should be required to protect it? This example addresses government storage of biometric data, but even private entities utilize biometric data for a variety of purposes, the most popular of which appears to be the use of fingerprints as ID cards for entry and timekeeping. But that requires the storage of biometrics, and as any evening news demonstrates, company-held personal data is rarely as safe as we would all like to presume. If entities are utilizing personal data, particularly biometric data, they need to maintain a robust privacy and security program to keep that data safe. Anything less opens the door to massive litigation risk and potential enforcement actions. --- Risa S. Katz-Albert

---

Potential Board Liability for Cybersecurity Failures Under Caremark Law

"Developments in Delaware's Caremark doctrine for breaches of fiduciary duty have paved a narrow path for plaintiffs to hold directors liable for failing to adequately address and oversee their company's cybersecurity and data privacy risks."

Why this is important: Cyberattacks are an ever-increasing threat to businesses around the world. As a company director, it is your responsibility to oversee your company's cybersecurity efforts. Failure to do so can catastrophically damage your company's finances and reputation. In the past 10 years, plaintiffs have tried to hold company directors personally liable for breaching their fiduciary duty by failing to adequately protect the company against cyberattacks. If the lapse in cybersecurity can be shown to be due to the company director's failure to properly prepare for cyberattacks, there is a narrow path for aggrieved parties to hold directors liable. To prove the directors' personally liable for a data breach or other cyberattack, a plaintiff must prove that (1) a board decision that resulted in a loss because that decision was ill advised or negligent, or (2) an unconsidered failure of the board to act in circumstances in which due attention would, arguably, have prevented the loss. Subsequent case law has refined this standard and provided greater guidance to plaintiffs seeking to hold company director's personally liable. The article outlines seven steps that company directors should take to ensure that they sufficiently address and implement cybersecurity and avoid being held personally liable. This includes the directors ensuring that they have sufficient cybersecurity training, that they have regular discussions regarding cybersecurity, they oversee the implementation of cybersecurity protocols, and that they regularly review the status of the company's cybersecurity protocols to ensure that they are up-to-date. Taking these steps, along with the additional steps outlined in the article, will provide company directors with a strong defense against plaintiffs who want to hold them personally liable in the event of a cyberattack on the company. **---** Alexander L. Turner

---

More GOP States Now Wagering on Vaccine 'Passports' Technology

"The technology had been touted by supporters as a way to facilitate safer reopening after pandemic-related shutdowns."

Why this is important: Many states previously opposed to "passporting" and barcoding vaccination status now support the concept. They want their residents to travel, go to events, etc. more easily. --- Hugh B. Wellons

---

6 Big Trends in the Cross-Border Payments Industry for 2022

"A strong global GDP and associated trade growth will keep accelerating the demand for cross-border payments, which is estimated to reach US$ 156 trillion by 2022."

Why this is important: Cross-border payments are transactions of currency that involve people or businesses in different countries. This article discusses six trends in the cross-border payments industry for 2022. I won't summarize them all here. Instead, I recommend the article, which provides an in-depth treatment of each while remaining easy to read and understandable. I want to briefly discuss two here because, in addition to being topics we have covered in prior issues of Decoded, they are topics I believe will emerge as two of the most significant financial and technology issues of this time. First is the increase of financial inclusion by digital remittances. An estimated 1.7 billion people globally are "unbanked," that is, they don't consistently have access to reliable banking services. However, 83 percent of adults in emerging countries own mobile phones. The growth of mobile wallets and e-payment options will help bring the unbanked under the tent of financial inclusion by providing them safe and reliable ways to save money, obtain loans, and participate in their economy. The second issue is the implementation of central bank digital currencies ("CBDCs"), a virtual or digital form of a country's official currency. Countries around the world are working to create CBDCs, including the U.S., and CBDCs will make cross-border payments faster and more cost effective. They also will play a role in geopolitics. China already has created and is testing its CBDC, the use of which it hopes will spread worldwide with the multitude of Chinese citizens working and traveling across the globe. It's also been said that China's CBDC is part of its ongoing bid to replace the U.S. dollar as the world's currency. --- Nicholas P. Mooney II

Applying mRNA to Healing Broken Bones

"Because the mRNA treatment effect appeared better than existing recombinant human BMP-2, mRNA 'provides an innovative, safe and highly translatable technology for bone healing,' the researchers wrote in the study."

Why this is important: I'll be brief, because I won't pretend to understand the science. The Mayo Clinic is experimenting with mRNA, the same core technology now used in many COVID vaccines. The twist is that the Mayo Clinic applies a specific mRNA to the injury site to encourage the body's production of a particular protein at that site. This protein speeds healing of broken bones. It already works in mice, but more study is needed. If successful, this could induce even major bone breaks to heal in a few weeks, instead of months. --- Hugh B. Wellons

---

This Plastic Dot Sniffs Out Infections Doctors Can’t See

"But if bacteria grow beneath the bandages, things can get dangerous."

Why this is important: This important medical advancement will detect an infection on an existing wound before a biofilm sets in by using sensors to detect elevated CO2 levels. The sensors are plastic dots that are secured under the clear plastic of the patient's dressing. Such sensors can be used to monitor the wound so that patients can avoid further infection. Some additional work is needed to fine tune the sensors to ensure that they do not emit false positive results. However, this may lead to using sensors to detect other chemicals such as sulfides, that may indicate the existence of an infection. These monitoring tools will assist patients with their recovery and may reduce the number of in-person medical visits. --- Annmarie Kaiser Robey

---

How an OTC Cough Med Could Serve as a Steppingstone for Creating Heart Rhythm Drugs

"The cough suppressant dextromethorphan, available over the counter, could activate a protein called sigma non-opioid receptor 1 to shorten the prolonged heart QT intervals in mice with a potential life-threatening form of inherited arrhythmia called Timothy syndrome."

Why this is important: Many drugs find new life serving an apparently unrelated purpose. Columbia University is studying the effectiveness of a common cough suppressant, dextromethorphan, to treat a particularly tricky heart arrhythmia. Like the broken bones result above, this seems to work on mice with few, if any, side effects. This is a long way from approval for humans. --- Hugh B. Wellons

---