SHARE:

Join Our Email List

View as Webpage

January 20, 2022

Welcome

Welcome to our first *Decoded* issue of 2022. This is our third year of publishing *Decoded* and as such, we felt it was time to reach back out to our readers for their thoughts and suggestions as we kick off the new year. Below, you will find a survey. If you have a moment, please take the time to let us know how we are doing. Do you like the content of *Decoded*? Is the timing of the publication appropriate? What else would you like see from our attorneys? Your input is what makes this publication helpful and insightful.

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*

EHR Vendor Breach Lawsuit Seeks Security Improvements

"Patient portal hacking incident last summer affected nearly 320,000."

Why this is important: On October 22, 2021, QRS Inc., a medical practice management system and electronic health record vendor, provided a HIPAA breach notification to the Department of Health and Human Services. QRS informed DHHS that over a three-day period in late August 2021, its patient portal was breached. The result of this breach was the potential exposure of 320,000 patients' personal health information. A putative class action lawsuit was filed in federal court in Tennessee alleging that the putative class representative and class members suffered damages related to actual identity theft as a result of the breach. In addition to damages, the putative class is seeking injunctive relief that would require QRS to implement a wide range of security improvements, including barring QRS from maintaining personal health information on a cloud-based database. This class action is based on the fact that QRS failed to implement "government-recommended" security measures and not statutory and

regulatory mandated security measures. Therefore, complying with governmental mandates is not enough to avoid litigation in the event of a breach. However, it is yet to be seen whether failing to implement recommended, but not required, security measures will result in the finding of liability. --- Alexander L. Turner

---

Cryptocurrency is Suddenly Everywhere — Except in the Cash Register

"While interest in crypto has exploded, few people are using it for its intended purpose: to pay for things."

Why this is important: Cryptocurrency is a buzzword in the financial world. Talk show pundits, celebrities, and financial advisers all espouse the value of the intangible digital currency. The idea of buying low and selling high, while typically associated with the stock market, now is equally associated with the cryptocurrency market. Interestingly, while 1 in 6 Americans now have traded, invested, or utilized cryptocurrencies, it is likely that such use was not for everyday purchases. More companies are attempting to make payment with cryptocurrency a viable alternative payment option. However, many companies that initially offered cryptocurrency payment options, such as Expedia, Dell, and Tesla, later removed that option due to lack of consumer interest. While seemingly inconsequential, such backtracking in availability of cryptocurrency as a payment option is emblematic of the key takeaway of the article: what is the future of cryptocurrency?

Retailers and individuals who want cryptocurrency to become a viable, alternative currency akin to the dollar, triumph the increase in use of cryptocurrency to pay for goods and services. However, the number of individuals actually doing so is next to nonexistent. In fact, financial experts will not even attempt to quantify the number of individuals using cryptocurrency to pay for such items as it is such a nominal amount.

On the other hand, there are the individuals who see cryptocurrency as an investment option akin to gold: a commodity to be bought as an investment rather than a currency to compete with the dollar. Entities that are normally risk adverse, such as retirement funds and 401(k) providers, have either invested in or allowed participants to invest in cryptocurrencies.

The American public is increasingly becoming involved in the cryptocurrency market, yet the instances in which one can pay for goods or services using cryptocurrency are limited. Until the future of cryptocurrency becomes more apparent, it is unlikely that there will be an increase in the number of vendors and outlets accepting cryptocurrency as a form as payment. --- Alyssa M. Zottola

---

BioNTech and London A.I. Firm Create 'Early Warning System' to Spot Dangerous New COVID-19 Variants Before They Spread

"In tests, the two companies said that their early warning system was able to pick up 12 of the 13 coronavirus variants that the World Health Organization has so far designated as potentially dangerous, doing so on average two months before the WHO reached that conclusion."

Why this is important: BioNTech, the original developer of the mRNA process used in the Pfizer vaccine, teamed up with a "big data" company to develop an early warning system for variants of COVID-19. In a recent test, they were able to pick up almost all of the variants the WHO identified as possibly dangerous. This may help Pfizer and others develop targeted vaccines before a variant infects many. As we know from the flu, this process is not perfect, and sometimes the variant you missed or the one you thought would not permeate the world is the one that does. It also may create a vaccine for a weakened variety that confers more immunity than risk. COVID-19 seems to mutate and spread much faster than the flu. mRNA vaccines can be developed much faster than traditional dead-virus vaccines traditionally used for the flu. BioNTech's efforts may help to offset this COVID-19 speed advantage. --- Hugh B. Wellons

---

Where does Nanotechnology Fit in Electrification?

"Nanotechnology has the potential to help revolutionize industries, especially when it comes to tackling environmental issues such as climate change."

Why this is important: Nanotechnology is playing an important role in fields from pharmaceuticals to electronics; here, the benefits of nanotechnology research and deployment are discussed as a key factor in the move to electrification. As consumer use, whether private or commercial, is such a large part of the climate impacts from energy use, it is crucial to design higher efficiency materials and products to aid in both reducing energy needs and more efficiently generating electricity. Strides have already been made, with nanotechnology being used to enhance electronics, insulation, coatings, HE light bulbs, transformers, and more. Ongoing nanotechnology research and development will lead to more efficient battery systems and generating units such as solar panels and wind turbines. However, nanotechnology research in the U.S. suffered from budget cuts and reduced funding generally through the early 2000s. With China currently leading the industry in nanotechnology research, it will be critical for the U.S., particularly through traditional research juggernauts such as NASA, to increase funding and support of nanotechnology research projects. --- Brandon M. Hartman

---

Teen Hacker Claims Ability to Control 25 Teslas Worldwide

"Hacker took control of Teslas in 13 countries."

Why this is important: Perhaps adopting the old adage "if you can't beat 'em, join 'em" – in 2015, Tesla's CEO Elon Musk began employing "crowdsourced security" to identify vulnerabilities in Tesla's security. Hackers who report bugs discovered in Tesla's system are rewarded with a "bounty" paid by the automaker itself. Bugcrowd.com reports that 600 bounties have been awarded thus far averaging $1,350.86 in the last three months. In 2017, Musk identified hacks to Tesla's fleet of vehicles as the company's "biggest concern."

This article is the latest report of Tesla's continuing technology vulnerabilities – describing how a 19-year-old security researcher was able to remotely unlock doors and windows, start cars, disable security systems, and blast music at full volume in select Teslas in 13 countries earlier – almost five years after Musk announced it was Tesla's "biggest concern." Tesla currently has 2.02 percent of the U.S. automotive market and has experienced record growth year over year (save 2019 when the world shutdown due to COVID-19), so why hasn't Tesla been able to address its technology vulnerabilities? As the electric car market continues to grow exponentially across the globe, it becomes ever more imperative that the weaknesses in the technology are corrected before the products go to market. --- Lori D. Thompson

---

Personalized Smart Guns, which Allow Only Verified Users to Shoot, May Become Available in US

"Smart guns are meant to prevent unauthorized people from firing guns in the hopes of keeping someone like a child or a convicted criminal from using the weapons."

Why this is important: Smart guns may revolutionize gun safety in the U.S. "Smart guns" are guns that will not fire without some form of electronic connection. Typically a "reader" with a finger- or palm-print programmed in may permit operation of the weapon. In some such devices, very close proximity to a fob, ring or bracelet permits gun operation. This article states that such smart guns soon will be available in the U.S. LodeStar Works, SmartGunz, and Biofire all are working on varieties of these ID systems. When working correctly, such guns reduce the risk of unauthorized firing of the weapon. This may greatly reduce, for example, school shootings, minors getting operable guns, criminals using stolen guns, and even law enforcement being shot with his/her own weapon in a scuffle. Law enforcement has and continues to experiment with this technology. A fine concept, it has faced prior challenges. Both of these methods require batteries, which die. The owner would have to keep up with that. Finger- or palm-print ID occasionally proves unreliable in wet or dirty situations. It also can be a problem in high stress, when the authorized operator may not be able to grab the gun in a perfect grip. The fob, ring or bracelet, if close enough, still may allow someone else to take the gun and fire it. If the fob, ring, or bracelet is stored with the gun, it's easy for someone else (a teenager?) to pick up both. Sometimes, these systems are not split-second, and they delay the ability to shoot. Fractions of a second count in many defense situations involving guns.

Most people who own guns consider at least some guns to be for home or personal defense. Anything that makes use of defensive guns more difficult or less reliable defeats that purpose. Many homes have at least two people trained to defend the home with weapons. These technologies, for the most part, do not allow multiple possible users. Some gun manufacturers, however, are intrigued by smart guns. They remove some of the potential liability that keep manufacturers up at night. Once the technology is practical, expect to see gun manufacturers at least offering it as an option. Some state legislatures may try to require this. Smart guns might not be ready yet for law enforcement, military or defense, but when the technology is better, smart guns will become common in the marketplace. Whether that technology can be required under the Second Amendment raises too many issues to discuss here. --- Nicholas P. Mooney II and Hugh B. Wellons

---

Crypto Scams are the Top Threat to Investors 'by Far,' Say Securities Regulators

"The annual survey of North American securities regulators urged investors to exercise caution before purchasing popular and volatile unregulated investments, especially those involving cryptocurrency and digital assets."

Why this is important: When cryptocurrency first came into the public sphere, it was viewed as a volatile, unsafe mode of payment often associated with criminal activity. As the public becomes more familiar and accepting of cryptocurrency, it has become a viable investment alternative to traditional investments. Typically risk-adverse groups, such as retirement fund operators, have even started to invest in cryptocurrency and provide their plan holders with the option of receiving part of their pension in cryptocurrency. The headline of this article, somehow implying that cryptocurrency lends itself more to scams or is a larger threat to investors, is disingenuous.

Many of the types of scams, such as "an offer of a high return with no risk" are also found in traditional investment schemes. Every day, individuals are scammed out of large sums of money by unwittingly falling for an investment opportunity that is too good to be true. To imply that investment in cryptocurrency is the only scenario in which an investor could be deceived into giving away large sums of money is absurd. However, what does separate cryptocurrency investments from traditional investments is the lack of regulation of cryptocurrency. While there certainly are "get rich quick" investment schemes outside of cryptocurrency, the federal regulations in place largely protect investors from these types of schemes. Cryptocurrency lacks these regulations, making it easier for bad actors to proliferate fraudulent schemes and attract unwitting investors. Additionally, many of the investment opportunities available in cryptocurrency are volatile and "extremely risky speculation with a high risk of loss." Moreover, the lack of a secure institution through which to conduct a transaction or to store the cryptocurrency poses a massive security threat. One of the biggest types of cryptocurrency-related crime in 2021 was theft of cryptocurrency, achieved largely through the hacking of cryptocurrency businesses.

The takeaway is that cryptocurrency, because of its novelty and lack of regulations, is somehow more likely to result in investors falling prey to Ponzi schemes or investment scams. I would argue that such implication is disingenuous and akin to fear-mongering: certainly the lack of regulations makes cryptocurrency investments an easier vehicle to perpetuate such a scam, but Ponzi schemes and similar scams occur frequently in traditional investment opportunities as well. However, that regulation is needed of the cryptocurrency market and cryptocurrency as a whole. While the lack of regulation is what appeals to many cryptocurrency consumers, if the goal of cryptocurrency advocates is to make cryptocurrency more appealing to the American public and to those favoring traditional investments, then regulation is a great way to achieve that goal. --- Alyssa M. Zottola

---

FDA Warns About Log4j Cybersecurity Vulnerabilities in Medical Devices

"As Apache Log4j is broadly used across software, applications, and services, medical device manufacturers should also evaluate whether third-party software components or services used in or with their medical device may use the affected software," the FDA said in the notice."

Why this is important: Cybersecurity breaches threaten businesses and individuals alike. The large increases in data breaches, ransomware attacks, and other cybersecurity events observed in 2020 and 2021 make this clear. A recently discovered vulnerability stemming from a widely used open source logging library poses a particularly serious threat. Apache Log4j is a software program broadly used in

many applications worldwide, but particularly in medical devices, possibly as many as 3 billion devices. It stores security-log and performance data critical to the operation of many of these devices. It was hacked in 2021, the hack announced in December. This vulnerability can allow third parties to substitute software code within devices to perform any number of unauthorized actions. It potentially impugns the security of software in any medical device connected to the internet. A solution suggested by the article is the "Software Bill of Materials" ("SBOM") proposed by a Biden Executive Order. While an SBOM may help to design safer software, it also may provide "bad guys" with a shopping list after the software is implemented. We recommend that manufacturers, healthcare providers and end-users of medical devices take proactive measures, such as performing security scans of devices and working to patch devices to address detected vulnerabilities. This is scary stuff! --- Brandon M. Hartman and Hugh B. Wellons

---

Why the Fed Hates Cryptocurrencies and Especially Stablecoins

"Powell told the House Financial Services Committee that the digital dollar project is moving forward."

Why this is important: Federal Reserve chair Jerome Powell recently testified on Capitol Hill regarding the efforts in the U.S. to develop a central bank digital currency ("CBDC"). Part of the incentive to develop a CBDC, he claimed, is to eliminate the use case in the U.S. for cryptocurrencies, especially stablecoins. Stablecoins are digital currencies that get their name from the fact that their value is pegged to the U.S. dollar and therefore do not suffer (or benefit?) from the volatility seen in other cryptocurrencies. Why is eliminating the use case for stablecoins an important goal? Powell would claim it is safety. Leaving aside the benefits of a U.S. CBDC, which Powell has questioned, the perceived danger of stablecoins is the claim that they still are an unregulated digital currency. While people may feel that using a stablecoin comes with the same safety measures as using the U.S. dollar, at its heart it is still a digital currency that operates outside the country's financial regulation system. Others claim the reason to eliminate stablecoins is the need to control. The fact that stablecoins operate outside the financial system is a feature, not a bug. They're concerned about "the loss of autonomy that occurs when permission to spend is implicit in the use of a currency." They want to avoid a system where digital transactions are slowed or stopped because they happen after hours or outside of a person's perceived usual spending habits. They worry that a U.S. CBDC could prohibit spending on items with which the government does not agree or could lead to temporary money, in which the government tries to spur spending by making money expire if not spent within a certain time period. Expect more to come on this soon. Several projects are underway in the U.S. to credit a CBDC or digital dollar, and efforts continue to be underway to regulate the entire cryptocurrency arena. --- Nicholas P. Mooney II

Gifts of DNA Tests Spur Paternity Surprises, Lawsuits

"DNA tests like 23andMe and Ancestry.com are leading to surprising paternity discoveries for some families."

Why this is important: Paternity discoveries are coming from an unlikely source – those at-home DNA test kits being purchased or gifted by well-meaning friends and family to explore their ethnic heritage, traits and unknown branches of the family tree. The story of the Johnson family's discovery that one of their children was the result of a fertility clinic sperm sample error highlights the unexpected legal issues that can arise from such discoveries. In that case, the mix-up of sperm samples was discovered 12 years after the child resulting from artificial insemination was born, and the legal ramifications appear to be limited to lawsuits against the fertility clinic by both the child's biological mother and biological father – but imagine a scenario where the discovery is made in the child's first year. Such discoveries may result in protracted custody fights; it is not difficult to envision difficult legal questions arising in other areas. For example, should executors and estate administrators be expected to utilize such kits to identify heirs, and what claims might arise in the future where heirs learn of their rights to inherit too late? As in the past, the law surrounding the use of new technology will continue to evolve and expand as the technology becomes more widely adopted. --- Lori D. Thompson

---

Please Fill Out Our Survey!

This survey will help us improve our efforts to provide you with timely and helpful information. If you have a moment, please provide feedback via our survey.

Click **here** to take the survey.
