SHARE:

Join Our Email List

View as Webpage

February 16, 2022

Welcome

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

Our Technology Practice Group gets together regularly to discuss trends in the industry, new case law and interesting developments. One of our attorneys, Alyssa Zottola, brought up the issue of arrests and seizures related to stolen cryptocurrency. She mentioned two articles she found of special interest -- one from the Justice Department and one from CNBC. If you are interested in some additional reading, you can find those here and here.

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*

Concerning Healthcare Data Breach Reporting Trend

"There has been a trend in recent years for HIPAA-regulated entities to wait the full 60 days from the date of discovery of the breach to issue notifications to affected individuals and the HHS, but recently growing numbers have taken the date of discovery as the date when the breach investigation has been completed, or even the date when the full review of impacted documents is finished."

Why this is important: HIPAA requires a covered entity to notify DHHS and affected individuals "without unnecessary delay" and no later than 60 days after the date of discovery of a data breach. But, when is the "date of discovery of a data breach?" Is it the day the breach is discovered, or is it the day that the investigation into the breach is completed? A recent trend has emerged where covered entities are waiting 60 days from the date of the completion of the investigation into the data breach to notify DHHS and affected individuals. To wait until 60 days after an investigation is completed creates a

significant compliance and liability risk. Even waiting the full 60 days after the date of discovery of the breach can still result in a claim for untimely notification. As we saw in our last edition of *Decoded*, a putative class brought a claim for untimely notification under HIPAA due to the covered entity waiting only 29 days from the discovery of the breach to notify affected individuals. DHHS has recognized this issue and clearly stated on its website that the 60-day notification period begins from the date of discovery of the breach and not 60 days after the completion of an investigation into the breach. Late reporting and notification risks a substantial fine, so strict compliance is a must. --- Alexander L. Turner

---

Breakthrough Device Program 'Far Exceeding' FDA Expectations After Record Year

"The agency designated 213 submissions as breakthrough devices last year."

Why this is important: Breakthrough devices are a relatively new FDA program that allows new, unique treatments to obtain early review and advice from FDA personnel during the process. This program began in 2015, but as the standards and processes have developed, more and more inventions qualify. The good news is it allows novel treatments to get to the market sooner. This encourages investment, because investors see a chance at an earlier return on the investment. Time will tell if these accelerated products create more negative results that time might have uncovered. This does demonstrate how the FDA is trying to adapt to better technology and new techniques that might quicken the regulatory path. We saw that clearly in the review of mRNA vaccines for COVID-19, and we may continue to see modernization in the near future. --- Hugh B. Wellons

---

The Five Things to Consider Before Regulating Cryptocurrency

"It is incumbent upon Congress to define the cryptocurrency industry and lay the appropriate regulatory groundwork before such decisions are made by existing regulators."

Why this is important: More than 16 percent of Americans invest in, trade, or use cryptocurrencies. There are over 30,000 Bitcoin ATMs nationwide. The market value of cryptocurrencies exceeded $3 trillion in November 2021. Regulation is coming to this space. It's a favorite topic among politicians lately. It seems every Congressional committee is holding a hearing on some aspect of the crypto space. (Even the Senate Committee on Agriculture, Nutrition, and Forestry recently held a hearing on regulating digital assets!) This space easily can be damaged or killed if someone who doesn't know how to turn on his or her computer or balance his or her checkbook imposes rules that have no basis in reality or the issues that need addressed. Likewise, a bias against this space will poison the process and the results. (A recent government report on stablecoins referenced their "risks" over 130 times, but only mentioned their "benefits" twice!) When Congress acts on this space, it must remember the questions asked in this article. Questions as basic as "What is a cryptocurrency?" must be examined and carefully considered. This isn't the time for turf wars between potential regulators (CFTC vs. IRS vs. SEC) or overlapping or inconsistent regulations that leave stakeholders with uncertainty. Cryptocurrencies and the fintech companies that issue them are a reality that is here to stay in a post-pandemic world where people feel safer conducting commerce digitally, Millenials and Gen Z'ers are becoming an active force in finance, and traditional and hierarchical ways of doing business are giving way to the quicker and less expensive. We need cryptocurrencies and fintechs to bring the unbanked and underbanked segments of our society under the tent of financial inclusion. We need egos checked at the Congressional door. This will take a scalpel, not a chainsaw. I've heard from people who are scared to death that Congress is going to attempt regulating this space, and they don't expect Congress to get it right. Regulation likely will happen, and when it does Congress needs to be careful and deliberate, listen to the stakeholders who operate in this space every day instead of lobbyists, pundits, or "experts," and focus solely on what will foster a robust digital asset environment that provides certainty, opportunity, and protection to those in this new segment of our financial system. --- Nicholas P. Mooney II

North Carolina Law Creates Regulatory Sandbox for Tech Companies

"Financial and insurance technology companies can now test out new products and services in a controlled space without worrying about certain regulatory barriers."

Why this is important: North Carolina is encouraging the development and growth of innovative financial and insurance technology products and businesses with the recent passage of the North Carolina Regulatory Sandbox Act. The Sandbox Act allows financial and insurance companies to test new products and businesses without the risk of running afoul of current regulations. A regulatory sandbox is a concept where a "safe space" is created in which businesses can test innovative products, services, business models and delivery mechanisms without immediately incurring all the normal regulatory consequences of engaging in the activity in question. The Sandbox Act provides a company with a limited amount of time to play around in the proverbial sandbox while under the strict supervision of the Innovative Council. Since its passage in October 2021, the regulatory sandbox has been used to create digital tokens for business-to-business payments. This is an exciting time for the financial and insurance industries to bring innovation in North Carolina. --- Alexander L. Turner

---

As Biometric Lawsuits Pile Up, Companies Eye Adoption with Care

"Many federal court cases were stayed pending that decision, but now that it's been decided, those paused cases will resume, Shifrin said."

Why this is important: Data privacy is a critical and underappreciated aspect of American society. Currently, there is not a nationwide biometric information privacy law, but such policies are increasingly being considered by state legislatures. As of this writing, Illinois, Washington and Texas have bioinformatics protection policies, with states such as Kentucky, Maine, Maryland, Massachusetts, New York and West Virginia considering bills similar to the Illinois Biometric Information Privacy Act ("BIPA"), which allows for an individual to control how their voices, fingerprints, facial scans, etc. are being used.

What sets BIPA apart from the policies in Washington and Texas is the private right of action afforded by BIPA. Individuals in Illinois can sue the company directly and recover damages; in Texas and Washington, the company would work with the State Attorney General to come to a resolution. Moreover, the Illinois Supreme Court recently ruled that injuries suffered by plaintiffs whose biometric data is misused are different than those compensable under the Illinois Workers' Compensation Act. In short, an employee alleging misuse of BIPA can seek redress for her injuries outside of the administrative remedies of the employment compensation act, vastly increasing the exposure for companies. Analysts predict that litigation will increase and settlement amounts will increase given the recent Illinois Supreme Court ruling.

Companies also should keep in mind that, even in states where there is not a defined biometric data protection policy, like BIPA, the company still could be liable for common law invasion of privacy claims if employee data (including biometric information) is not properly protected.

Companies need to start (if they have not already done so) reexamining their policies regarding the protection of their employees' data, and how their policy comports with the laws of the state/states in which they conduct business (even if there is not a biometric data protection policy enacted). While such a task is complicated by the fact that there is not a uniform biometric data protection policy across the United States (nor is there a biometric data protection policy present in each state/territory), failing to comply with the policy of that particular state or territory opens up the company to potentially devastating legal liability. --- Alyssa M. Zottola

---

Live Human Tendon 3D Printed by Scientists with New 'Cryo-Bioprinting'

"According to the scientists, their technique also yields tissues that are more robust and versatile than those produced via conventional bioprinting, particularly when it comes to those anisotropic in nature, thus they say it could now find regenerative medicine, drug discovery, or personalized therapeutic applications."

Why this is important: We've transplanted pig tendons, ligaments, heart valves, and even a heart from animals to humans, and we've made plastic/human tissue structures to aid healing of large wounds, but can we actually build a structure by bioprinting that will stay together under pressure, and be able to

contract and stretch? Harvard Medical School and Sichuan University seem to have developed a means of making tissue, freezing it, and connecting it in order to provide a synthetic tendon that actually works. How long before you can replace tendons to run faster or jump higher? How will sports regulatory agencies test for and control that? --- Hugh B. Wellons

---

No Pre-Emption of Illinois Biometric Data Privacy Lawsuits from Workers' Comp

"Macy's knocks out some claims, TikTok settlement held up."

Why this is important: The landscape for businesses operating in Illinois continues to be tenuous with the latest ruling from the Illinois Supreme Court. We previously reported that the Illinois Biometric Information Privacy Act ("BIPA") has proven to be a liability minefield. It requires any company to obtain informed consent, as defined by the statute, and a written release in advance of capturing any biometric information. Security check points and mandatory temperature check stations during COVID-19 without obtaining a signed release in advance have already provided fodder for class actions that are pending there. This month the Illinois Supreme Court, in the case of *McDonald v. Symphony Bronzeville Park, LLC*, dealt a blow to employers who might seek shelter from the wide-reach of BIPA by raising the workers' compensation bar. In this case, a nursing home employee sued her employer who required her to check in and out from work using a simple fingerprint system that logged the time she entered and exited. The employee sued alleging that the process violated BIPA because she was never provided with the specifics as to how her biometric information would be utilized and never signed a release. The nursing home asserted that her claim was barred by the Workers' Compensation Act, which provides the exclusive statutory remedy for work-related injuries. The Illinois Supreme Court disagreed, noting that the language in BIPA evidences that the Legislature considered employers within its scope. Significantly, a proposal is currently pending in the Illinois Legislature that may effectively overturn this result. However, without a legislative fix, the floodgates for class actions in Illinois against employers there are wide open. What is happening in Illinois should be a wake up call to all businesses to closely monitor any legislative proposals addressing biometric data in any state where they operate. --- Lori D. Thompson

---

A Florida Home to be Auctioned as an NFT has Attracted More than 7,000 Potential Bidders

"The Gulfport, Fla. house will be auctioned with a starting price of $650,000, through a partnership between real estate companies Propy and Heckler Realty."

Why this is important: NFTs have made large splashes in the news at several points in the past 12 months. From famous digital artists selling pieces for $69 million at auction to digital real estate being sold within virtual reality gaming worlds, the general public has had many occasions to ponder exactly what this technology is and what makes it have any real value. Now, a real property existing in the real world is going to be auctioned in Florida as an NFT. While the initial reaction to this news might be dismissive, the implications of utilizing elements of NFT technology for sale of real assets such as property present both opportunity and problems. The ability to incorporate clear record of ownership and other title-relevant data within the blockchain of the NFT could provide an easier mechanism for digitizing property records, which could in turn lead to future title searching being made a much simplified process. Though, perhaps vehicles or other such personal property might be a better, less risky, place to start developing such a digital record system for titles. Anyone interested in utilizing NFTs for the transfer of real property should also consider carefully that NFTs allow for a percentage of future sales to be reserved by a seller directly within the blockchain of the NFT, which means these reservations will perpetuate as a part of all future sales. Until or unless the legal system addresses this issue with respect to real property sold via an NFT, interested parties and their counsel should be aware of this issue and carefully examine the stipulations placed on and within an NFT to real property. --- Brandon M. Hartman

---

Judge Proposes Dismissal of Practicefirst Data Breach Lawsuit

"In July 2021, Practicefirst began notifying over 1.2 million individuals of a healthcare ransomware attack targeted at the medical billing, coding, and practice management vendor that potentially exposed protected health information (PHI) and personally identifiable information (PII)."

Why this is important: Speculative future harm does not convey standing to victims of a data breach, so says U.S. Magistrate Judge Michael Roemer of the Western District of New York in his Recommendation and Report to the presiding District Court judge in a data breach action against Practicefirst. The basis for Judge Roemer's recommendation is the U.S. Supreme Court's recent holding in *Ramirez v. TransUnion* in which the Supreme Court stated that data breach victims must demonstrate an actual injury proximately caused by the defendant in order to recover. The case currently pending in the Western District of New York is a putative class action against Practicefirst, a medical management company, related to a data breach in December 2020. The putative class asserted in its class action complaint that they allegedly suffered actual injuries as a result of the breach in the form of diminished PHI value, a violation of their privacy rights, and the possibility of future harm due to the increased risk of identity theft. However, Judge Roemer recommended the dismissal of the putative class' complaint due to a lack of standing as a result of the plaintiffs' failure to allege an injury-in-fact. In our last edition of *Decoded*, we discussed the viability of claims of diminished value of personally identifiable information and protected health information as an injury-in-fact. Now we have an answer to whether those claims are viable. Judge Roemer stated that, "[t]he complaint contains general and conclusory allegations that PII/PHI is a 'valuable commodity' on the 'cyber black-market' and that 'many companies now offer consumers an opportunity to sell this information to advertisers and other third parties'. However, plaintiffs do not allege that they attempted to sell their personal information and were forced to accept a decreased price, nor do they allege any details as to how their specific, personal information has been devalued because of the breach." Judge Roemer also stated that dismissal is appropriate because the plaintiffs failed to allege an imminent or certainly impending risk of future harm because they did not allege that the breach was targeted to expose or copy their confidential information, that the breach resulted in misuse, and because an assertion of a mere exposure of PII and PHI without targeted exposure or actual misuse did not show that there was a substantial risk of future identity theft or fraud. The Court also rejected the plaintiffs' privacy claim because, as pled, it did not satisfy the elements of the common law claim. What Judge Roemer's Recommendation and Report shows is that while data breaches are becoming more common, the courts are becoming stricter regarding what claims can be brought and what constitutes an actual injury-in-fact. --- Alexander L. Turner

---

Doctors: Cancer Patients Cured a Decade After Gene Therapy

"They say the two examples show the treatment, called CAR-T cell therapy, can attack cancer immediately, then stay inside the body for years and evolve there to keep the disease at bay."

Why this is important: Cancer treatment by "Car-T" has been around for over a decade. We've addressed it before. It is used currently to treat serious cancers that are resistant to other treatments. Car-T involves removing a sample of the patient's blood, withdrawing a certain amount of the patient's immune cells, revising/training those cells to attack the cancer, and inserting the revised cells into the body. When it works, the new cells multiply and search for and destroy the cancer. The article talks about two very successful patients who have/had a cancer that is deadly. In their cases, Car-T was performed 10 years ago, seemed to eliminate the cancer, and apparently still is eliminating or preventing the cancer today, with minimum or no side effects. The legal and societal issue is this: Car-T is very expensive -- hundreds of thousands of dollars. The cost will come down, but it is by nature personal medicine. That always will cost a lot, because it is personalized. As a result, it is doubtful that it will be available to everyone. As we move toward single-payer medicine, to what extent will we cover more expensive therapies involved in personalized medicine? Who decides?

This also illustrates a second question about complicated medicines. What is the long-term effect? Car-T has been around long enough to demonstrate that it usually has few, if any, side effects. Scientists believed that 10 years ago, but they were not certain. Next edition, we will address situations where the long-term effects still are unknown. That creates interesting legal concerns. --- Hugh B. Wellons

---

Why U.S. Minority Communities May Turn to Cryptocurrencies to Pay Their Bills

"Recent research finds that 24% of cryptocurrency owners are Hispanic, versus 16% of all U.S. adults."

Why this is important: Cryptocurrencies are often heralded as a tool for financial inclusion for the unbanked and underbanked. This article suggests that may be true. Several studies discussed in the article reveal that minority communities are in need of alternative payment options. They may be turning to cryptocurrency. While 16 percent of U.S. adults identify as Hispanic, 24 percent of cryptocurrency owners identify as Hispanic. Part of the reason for this disproportionately high number may be the enthusiasm of the crypto boom in Latin America, and part may be the ease that crypto allows Hispanic Americans to send money to Latin American countries. Asian, Black, and Hispanic adults are more likely than white adults to have used cryptocurrency. Studies suggest one of the reasons may be the search for a better payment system. Crypto owners have used Western Union, check cashing services, payday loans, and auto title loans in larger percentages than U.S. adults overall. At bottom, data confirms the belief that cryptocurrencies bring financial inclusion to people who otherwise would be unbanked or underbanked, and that should not be forgotten amid the call here in the U.S. to regulate cryptos and actions abroad to regulate or attempt to ban them. --- Nicholas P. Mooney II
