SHARE:

Join Our Email List

View as Webpage

February 3, 2022

Welcome

Welcome to our second *Decoded* issue of the year! In addition to discussing a wide variety of trending technology topics in this newsletter, we like to employ audio and video to reach our clients. Is there a webinar you would be interested in attending? Are there topics you would like addressed in an audio and/or video format? We have that capability and would welcome the opportunity to address issues that interest you. Just email either one of us and let us know your thoughts.

Also, we want to hear what you think about this publication. Have you taken our survey? We are interested in what you think about our content, the timing, the way you receive the information, and where we can improve. Click **here** or check out the link at the bottom of this e-newsletter.

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*

BioPlus Specialty Pharmacy Faces Lawsuit Over Healthcare Data Breach

"Florida-based BioPlus Specialty Pharmacy allegedly failed to safeguard PII and notify patients of a healthcare data breach that impacted 350K, the lawsuit claimed."

Why this is important: Another day, another data breach of a healthcare provider that resulted in the unauthorized access of patients' personally identifiable information ("PII") and protected health information ("PHI"). In this case, BioPlus Specialty Pharmacy in Florida suffered a data breach between October 25, 2021 and November 11, 2021 that impacted approximately 350,000 BioPlus customers. BioPlus is now embroiled in a class action lawsuit related to the breach. This is a common result of a

healthcare related data breach, large or small. What is interesting about this case are the claims the putative class are asserting and the damages they are seeking. In addition to claiming that BioPlus was negligent in allowing its computer system to be breached, the putative class is also arguing that BioPlus failed to timely notify the affected customers of the breach. It is unlikely that the putative class will be able to recover on this claim because BioPlus notified the affected customers within 29-days of the discovery of the breach, which is well within the HIPAA mandated 60-day notification deadline. In addition to seeking the usual data breach damages of costs, expenses, and lost time related to protect themselves against the breach, the putative class is also seeking to recover possible future damages, including for "fraudulent charges, medical procedures ordered in patients' names without their permission, and targeted advertising without patient consent." Because these possible future events are speculative, it is unlikely that the putative class will be able to recover these damages. But, those are not the most creative damages the putative class is seeking. They are also requesting an award of damages for the diminished value of their PII and PHI due to the breach and believed sale of this private information on the black market. This is an interesting argument to make because these damages will be incredibly difficult to prove. They would first be required to prove that their PII and PHI were subsequently sold on the black market following the breach. After proving that the information was sold by the bad actors, the plaintiffs then have to show that their PII and PHI suffered a diminishment in value. If there is no legitimate market, or if the members of the putative class are not intending to ever sell their PII and PHI, then there can be no diminishment in value because the PII and PHI had no intrinsic value in the first place. If there is a legitimate market for this information, the putative class would have to prove that this market even cares about where else this information may have been sold. Only then does the actual calculation of the diminishment in value of the PII and PHI become relevant. How you calculate the diminishment in the legitimate value of information that is intrinsically private and for which there may be no legitimate market is a thought-provoking problem that would require expert testimony. At this time, based on the limited information we have on the putative class' argument in favor of these damages, it would appear that the putative class would not be able to recover damages on the alleged diminished value of their PII and PHI because there would be no way to quantify what the value of that information is pre- and post-breach. What this case shows is that class action plaintiffs' counsel are getting creative and advancing new arguments and damages claims in an attempt to increase their recoveries, either through settlement or trial, in data breach cases. Whether these creative arguments will pay off has yet to be seen. --- Alexander L. Turner

---

US Commerce Dept Says Chips Shortage to Persist, Will Review Some Prices

"Median inventory for consumers for key chips has fallen from 40 days in 2019 to less than 5 days in 2021."

Why this is important: Bad news! The current chip shortage likely will persist. This creates shortages in many electronic products, from toasters to automobiles to laptops and even supercomputers. Raw material shortages, transportation challenges, just-in-time deliveries, greater employee sick days, the Great Resignation, rising chip demand, and other things are conspiring to exacerbate an existing problem with computer chip availability. And, shortages in these products drive down revenue and, well, almost everything else. Hard to deliver something if you cannot get a truck! But the U.S. Congress is investigating this now, so how could a solution be far behind?! Oh yes, that'll fix it! **---** Hugh B. Wellons

---

How to Protect Against Biometrics-Related Class-Action Lawsuits

"In addition to BIPA, regulatory laws have been passed in Texas, Washington, California, New York and Arkansas."

Why this is important: Illinois has long been the front-runner regarding regulating use of biometric data through the Illinois Biometric Information Privacy Act of 2008 ("BIPA"). Now Texas, Washington, California, New York, and Arkansas have joined the biometric regulating party, to varying degrees. This topic area, much like so many other data privacy topic areas, is becoming a patchwork of state-specific requirements that arguably must all be followed in the context of a national organization using biometric data. Further, with the increased reliance on technology driven by the ongoing COVID-19 crisis, technology used to ensure fair test taking is coming under fire for its use of biometric data evaluation. The increasing utilization of biometric technologies and the increasing regulation of that use are colliding, and businesses are left to fit together the puzzle pieces as they shift. --- Risa S. Katz-Albert

Cryptocurrency Money Laundering Climbs 30% in 2021

"In 2021, cyber criminals laundered over $8.6 billion worth of digital currencies."

Why this is important: This has been a problem for almost a decade. Most digital currencies are legitimate. Digital currencies, however, as soon as they were created, offered anonymity. Anonymity is exactly what money laundering covets! These currencies provide excellent vehicles to move money from one place to another, with no government supervision and few restraints. There are good reasons to move money surreptitiously. Unfortunately, there are plenty of bad reasons as well. This "bad" represents a small percentage of all cryptocurrency transactions - probably less than 1 percent - but it is a lot of money, approximately $900 million last year! This helps to support drug sales, theft, cybercrime, etc. --- Hugh B. Wellons

---

IMF Urges El Salvador to Abandon Using Bitcoin as Legal Tender

"Additionally, the report urged Salvadorian authorities to refine the scope of its Bitcoin law by removing Bitcoin's status as legal money."

Why this is important: El Salvador announced last year that it was adopting Bitcoin as legal tender, alongside the U.S. dollar. It also launched a national digital wallet called Chivo and provided citizens with free Bitcoin as incentive to create their wallets. The IMF criticized this move almost immediately and has continued to encourage El Salvador to reverse course and drop Bitcoin as legal tender. The price of Bitcoin is down almost 50 percent from its high in November 2021. El Salvador responded to this drop by doubling down on Bitcoin and purchasing an additional $15 million. The drop in price brought renewed criticism by the IMF, this time emphasizing that Bitcoin brings large risks to financial stability, financial integrity, and consumer protection. El Salvador continues to be bullish on Bitcoin. However, it has been attempting to secure a $1.3 billion loan from the IMF, and those attempts have stalled. Jettisoning Bitcoin as legal tender might break the logjam on that loan. We should see in the near future whether El Salvador will continue its plan to use Bitcoin as legal tender or whether the drop in price and the promise of a $1.3 billion loan from the IMF will convince it to change its mind. --- Nicholas P. Mooney II

Amy Klobuchar Leads Her Final Assault on Big Tech's Power

"Antitrust reform is on the horizon, and tech is spooked."

Why this is important: Amy Klobuchar is leading the way to restrict what amounts to self-dealing by the big tech information providers/managers, Google, Facebook, Twitter, etc. She also wants to go after them for antitrust violations, because they allegedly are monopolies. She will find many like minds across the aisle for this. --- Hugh B. Wellons

---

Mecklenburg County Mistakenly Identifies Unvaccinated Employees in Email

"In a follow-up email to county commissioners, county manager Dena Diorio said the email was not a violation of HIPAA — a federal law that created national standards for protecting sensitive, personal health information — and that the county would send out an apology."

Why this is important: Recently, *Decoded* published an article addressing the issue of an employer's duty to protect their employees' protected health information ("PHI") from a data breach in the age of COVID-19. Unfortunately, Mecklenburg County, North Carolina did not adequately protect their employees' COVID-19 related PHI. Mecklenburg County has a vaccine mandate for its employees. As the deadline for providing the county with proof of vaccination approached, the county decided to send a reminder email to its employees. However, instead of sending the reminder email to all employees,

Mecklenburg County inadvertently sent the email to only those employees who had not yet submitted proof of being fully vaccinated against COVID-19. The result was a possible disclosure of those employees' PHI by identifying them as possibly not being vaccinated. While the County Manager, Dena Diorio, is correct that this was not a HIPAA violation, that may not absolve Mecklenburg County of liability. Even though HIPAA does not apply to Mecklenburg County, the county still has a statutory duty, pursuant to the ADA, and a common law duty to safeguard its employees' PHI. This self-inflicted data breach and disclosure of some of its employees' PHI by Mecklenburg County may still result in litigation and a finding of liability. For ways to safeguard your employees' protected health information, please see our previous article Protecting Employees' Private Health Information from a Cyberattack in the Age of COVID-19. --- Alexander L. Turner

---

Have You Filled Out Our Survey?

There is still time to fill out our survey and help us improve our efforts to provide you with timely and helpful information. If you have a moment, please provide your feedback.

Thank you!

Click **here** to take the survey.
