SHARE:

Join Our Email List

View as Webpage

May 26, 2022

Welcome

Welcome to the tenth issue of *Decoded* for the year.

To kick off this issue, we want to congratulate many of our attorneys and the firm for recently receiving the 2022 Distinguished Pro Bono Award from Legal Aid of West Virginia.

The Distinguished Pro Bono Award recognizes a lawyer or law firm whose pro bono efforts in a given year have gone "above and beyond" the call of duty and are deserving of special recognition. In 2021, Spilman attorneys used their professional talents to donate more than 70 hours of pro bono assistance to Legal Aid of West Virginia clients, with significant time spent helping families adopt children.

This is a much deserved recognition for the time and effort many of our colleagues put in all year. Congratulations!

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*

House Subcommittee Debates Device Remanufacturing Definition, Sends User-Fees Bill to Next Stage

"Proponents of the remanufacturing bill are looking to better distinguish between medical device remanufacturing, and servicing or repairs, saying it would improve patient safety."

Why this is important: Getting a simple oil change on a vehicle is certainly not the same as rebuilding the car after an accident. In some instances, repairing accident damage may be significant enough to result in a vehicle being reclassified as "salvage" on its title documents – or otherwise voiding a manufacturer warranty. The title is branded to put future buyers on notice that significant alterations have been made to the vehicle and that it may not work the same as before the accident. The same guiding principles should apply to medical devices.

In 2018, an FDA report found that most complaints regarding the inadequate servicing of medical devices were actually complaints regarding remanufactured medical devices. In an effort to advance patient safety, new bills are currently working their way through the House that seek to differentiate between what constitutes servicing and remanufacturing medical devices. By clearly defining these actions, Congress not only wants to ensure medical facilities and the public are aware of the status of the equipment being used to treat patients, but that the remanufactured equipment will work as intended. This is a critical step in protecting consumer safety and providing clear guidance for manufacturers and third parties in the medical device industry. The final definition language selected will have significant implications on future legislation.

The bills also address the issue of timely servicing of medical devices. While medical facilities in large metropolitan areas are able to have broken equipment fixed relatively quickly, that is not the case in rural areas or even smaller cities. Congress wants to fix that by legislating that manufacturers ensure that medical devices are able to be timely repaired in the event of a problem in order to limit equipment downtime. However, some Representatives are concerned that the requirement is too strict and that the bill "as written is problematic."

These are examples of patient safety and medical technology legislation that Congress is currently debating. Another piece of patient safety technology legislation that is currently working its way through Congress is the PATCH Act. The PATCH Act addresses the dangerous issue of known cyber vulnerabilities to medical devices that we have discussed in previous editions of *Decoded*. Please be on the lookout for our next edition of *Decoded* where we take a deep dive into the PATCH Act and discuss the implications of that proposed legislation. --- Alexander L. Turner and Brian H. Richardson

---

CA Health Plan Faces Lawsuit After Cybersecurity Incident Linked to Hive Ransomware

"According to VentureBeat, Hive ransomware claimed responsibility for stealing 850,000 personally identifiable information records from the health plan."

Why this is important: The lawsuit filed against Partnership HealthPlan of California ("PHC") alleges it failed to design its computer network to prevent ransomware attacks. However, the interesting thing is that PHC hasn't acknowledged than a ransomware attack has even taken place. Hive ransomware, a group responsible for other healthcare-based cyberattacks, has claimed that it stole 850,000 records from PHC that contain individuals' personally identifiable information. PHC has not provided notification to HHS or the affected individuals, even though the time for doing so may have run. According to the article, PHC hasn't taken any steps to acknowledge that a ransomware attack even took place. The lawsuit was filed earlier this month and PHC's response likely isn't even due yet. When it's filed, the response should shed light on the question of whether an attack took place and, if so, its magnitude. This article discusses how choosing not to respond to a ransomware attack or other type of data breach (if indeed one did happen here) won't necessarily prevent a later lawsuit. In fact, it may make things worse. --- Nicholas P. Mooney II

FDA Needs Testing Enforcement Discretion Policy to Improve Crisis Response, GAO Finds

"Acting on a request from Congress, the GAO looked at FDA's actions to help make COVID-19 tests available, the number of tests it authorized, how often it exercised enforcement discretion and what post-market monitoring activities it implemented."

Why this is important: This opinion states that the FDA needs both enforcement power and deeper protocols in how it quickly measures the effectiveness of tests and authorizes tests available to the public. Some locations still are short on tests. In the next pandemic, we need to evaluate and put into

the market legitimate tests as quickly as possible. Legally, this is not necessarily part of the FDA's mission. Tests are not usually considered "drugs." But, who else can do this? --- Hugh B. Wellons

---

NSA, Allies Issue Cybersecurity Advisory on Weaknesses that Allow Initial Access

"The Cybersecurity and Infrastructure Security Agency, the National Security Agency and the FBI, along with allied nations, published a Cybersecurity Advisory to raise awareness about the poor security configurations, weak controls and other poor network hygiene practices malicious cyber actors use to gain initial access to a victim's system."

Why this is important: Recently, the Cybersecurity Infrastructure Security Agency, the National Security Agency, and the Federal Bureau of Investigations, along with certain U.S. allies, published the Cybersecurity Advisory. The Advisory seeks to provide a warning about some of the vulnerabilities that cyberattackers exploit to gain access to a company's systems. Some of the vulnerabilities are as simple as the failure to use multifactor authentication and weak password procedures. The Advisory provides an extensive list of examples that attackers use. Companies would be well-served to compare this list to their own practices to see how they measure up and where changes need to be made. --- Nicholas P. Mooney II

LabCorp Becomes First Company to Get EUA for Direct-to-Consumer Test for Flu, RSV, COVID-19

"The FDA shared details of the emergency use authorization on the same day that LabCorp disclosed the launch of an at-home sample collection device for diabetes-risk testing."

Why this is important: The wider public looks to have a growing toolkit for detecting infection by respiratory viruses, a crucial tool for early prevention of the spread of these diseases. LabCorp has received emergency use authorization from the FDA for an at-home test kit for collecting nasal swab samples to send in for testing as the presence of multiple viruses, including influenza A and B, respiratory syncytial virus, and SARS-CoV-2. These advances to bring tests such as this to the market are important in bringing to fruition the convenience of fully testing at-home for these all too common types of viruses. However, as the United States enters summer and flu season again approaches, these at-home tests will be another tool for those experiencing respiratory virus symptoms to utilize for determining if they are experiencing an illness and should limit contact with others for a period. --- Brandon M. Hartman

Why this is important: LabCorp received EU approval to market an over-the-counter swab-kit (actual analysis performed at a lab), that tests for multiple pathogens, including flu and COVID. This will raise the tort stakes (three ways to get it wrong!). The fact that the test sells over the counter, with the sample obtained at home, while the analysis is performed at a lab, makes this similar to other tests now available, such as the myriad of at-home colon cancer screens. Besides tort concerns, it will be interesting to see how well this is accepted for negative proof. --- Hugh B. Wellons

---

How Big Data Analytics Can Support Preventive Health

"Big data analytics provide enhanced data-related capabilities to healthcare providers, which they can use to support large-scale goals and health outcomes."

Why this is important: "Big data" analytics uses powerful computers (not your typical PC!) to find patterns that are not otherwise noticeable. Researchers are using these same tools to discover patterns in serious illnesses and conditions. Because many such maladies are better treated, or even cured, early, finding early indicators increases the chance of survival. For example, what if two other common maladies are often an early indication of a deadly cancer? Wouldn't you want to know that? This will raise questions about who owns the analysis of readily available data. It also may impose on general practitioners a higher duty of care in terms of noticing the early indicators and notifying the patient. --- Hugh B. Wellons

---

Mastercard's Latest Test Would Make Credit Cards Obsolete by Letting Customers Use Their Faces and Finger Prints to Pay in Stores

"Trials for the new payment options kicked off in Brazil, with Mastercard collaborating with a Brazilian supermarket chain and Payface, a company that specializes in facial recognition software to enable digital payments."

Why this is important: Mastercard is seeking to expand the ways which consumers can pay for purchases. The company is in the process of testing technology that would allow an individual to submit payment by waving their hand over a scanner or through facial recognition. They envision these technological advancements as a means to do business in the metaverse and to provide consumers with access to their payment information without having the credit card in hand. The consumer data would be stored in a database that can be accessed by retailers through biometric markers. The technology has the potential to facilitate the speed of transactions resulting in shorter checkout lines. Since sensitive information such as the biometric data and the consumer information will be stored in a database, it is imperative that adequate security precautions are in place. Should the security measures fail, consumers will have more than a credit card number compromised. --- Annmarie Kaiser Robey

---

SolarWinds Data Breach Lawsuit Takeaways for CISOs

"A lawsuit alleges SolarWinds did not take adequate actions to prevent a data breach."

Why this is important: In a prior issue of *Decoded*, we previously discussed four top concerns for Chief Information Security Officers (CISOs). The article discussing the SolarWinds breach adds another concern to that list. In 2019, Russian Foreign Intelligence Services breached SolarWinds' networks. Because the company's software was widely used by the federal government, the breach allowed the attackers to access the networks of several federal agencies. SolarWinds' stock price plummeted, resulting in a lawsuit by SolarWinds shareholders. The lawsuit names several company officers and alleges they were negligent in preventing the attack and participated in a "fraudulent scheme" to mislead investors about the company's security practices. This article contains a lengthy discussion about the significance of the lawsuit as seen by several industry players. One significant point to note: although the court dismissed the plaintiff's claims that the then-CEO was personally liable, the court didn't dismiss similar claims against the company's CISO. The attempt to hold executives personally liable is certain to have many CISOs and others in the industry watching this lawsuit. --- Nicholas P. Mooney II

Seth Green Loses $200K Bored Ape Yacht Club NFT in Phishing Scam

"In a subsequent tweet, Green said he was trying to buy an NFT -- a Gutter Clone, a spinoff from a popular collection called Gutter Cats -- and connected his wallet to the site, which ended up being a scam website."

Why this is important: This unfortunate circumstance serves as an important reminder of the pernicious nature of phishing and other e-scams. In short, actor and comedian Seth Green was attempting to purchase another NFT to add to his collection and ended up connecting his wallet to a site that was in fact a scam website. Unfortunately, his wallet contained several other rather valuable NFTs. These were stolen as a part of the scam, and the very nature of crypto and NFTS being highly decentralized makes the possibility of having these returned very unlikely. While the majority of us may not hold valuable NFTs that are at risk of theft, we all face digital scams on a mostly day-to-day basis. These scams can be quite elaborate, and diligent care must be taken to prevent theft of personal, work, or employer data via an inadvertent download of an infected file or a click-through to a well-designed phony website such as what unfortunately happened here. --- Brandon M. Hartman

---

Internet of Behavior Grows but Can the Industry Get Ahead of Public Misgivings?

"Unfortunately for the nascent industry, the fullest example of how the Internet of Behaviors can operate is autocratic China's social credit score program."

Why this is important: "Internet of Behaviors" is a nice term for collecting, saving, quantifying, and rewarding (or penalizing) certain behaviors. China infamously began this practice years ago and uses it to correct any individual's behavior that the state deems unfavorable. It requires extensive spying on every citizen and apportions benefits based on each citizen's "score" of behaviors. Now, some political and business interests are supporting the use of ESG (environmental, social, and governance) scores to measure compatibility and "risk," in terms of doing business with individuals and businesses. --- Hugh B. Wellons

---

Share Tweet Share

This is an attorney advertisement. Your receipt and/or use of this material does not constitute or create an attorney-client relationship between you and Spilman Thomas & Battle, PLLC or any attorney associated with the firm. This e-mail publication is distributed with the understanding that the author, publisher and distributor are not rendering legal or other professional advice on specific facts or matters and, accordingly, assume no liability whatsoever in connection with its use.

Responsible Attorney: Michael J. Basile, 800-967-8251