March 3, 2016

ENFORCEMENT + LITIGATION

First Data Security Enforcement Fine Levied by CFPB against Dwolla Inc. for $100,000

Wading into the foray of enforcement of data security practices, the Consumer Financial Protection Bureau (CFPB) yesterday hit Dwolla Inc., an online payment processor, with a $100,000 fine for a myriad of violations of the Consumer Financial Protection Act of 2010.

Specifically, the CFPB, in a scathing order, outlined in detail the facts that Dwolla, who at the time of the order had approximately 650,000 users and was transferring up to five million dollars per day, misrepresented the level of its security practices to consumers from 2011 to 2014. The allegations include falsely claiming that its security practices "exceeded" or "surpassed" industry standards, falsely claiming that consumers' information was securely encrypted and stored, both in transit and at rest, that its platform was safer than credit cards, and that it stored consumers' information "in a bank-level hosting and security environment," and "encrypts data using the same standards required by the federal government," all of which were false according to the CFPB.

In fact, the CFPB states that Dwolla failed to adopt security policies, failed to adopt a written information security plan, failed to implement a risk assessment, failed to train employees, and even encouraged consumers to submit sensitive information, including Social Security numbers via unencrypted email.

In addition to paying the $100,000 fine, the CFPB is requiring Dwolla to stop misrepresenting its data security practices, train its employees, fix the weaknesses on its web and mobile applications, and implement security practices. Another federal agency to keep an eye on to enforce data security practices of financial institutions.

— Linn Foster Freedman

Jason Pierre-Paul Sues ESPN and Adam Schefter for Tweeting Photo of Medical Records

New York Giants defensive end Jason Pierre-Paul has filed suit against ESPN and ESPN reporter Adam Schefter for violations of Florida Statute § 456.057 and for invasion of privacy arising from a tweet containing a photo of Pierre-Paul's medical records.

As many of you no doubt remember, Pierre-Paul was hospitalized at Jackson Memorial Hospital in Miami, Florida, on July 4, 2015, after suffering a serious injury in an accident involving fireworks. Four days later, Schefter tweeted a photo of Pierre-Paul's medical records to confirm that Pierre-Paul had his

right index finger amputated. At the time of the tweet, Schefter had over four million followers.

Florida Statute § 456.057(7)(a) provides that medical records "may not be furnished to...any person other than the patient, the patient's legal representative, or other health care practitioners and providers involved in the patient's care or treatment, except upon written authorization from the patient." Hospital employees almost certainly violated this requirement when they provided the records in question to Schefter.

Jackson Memorial Hospital was not named in this lawsuit, but it is likely that Pierre-Paul previously sued the hospital separately. On February 5, 2016, the hospital issued a statement to the effect that two employees responsible for leaking the medical records had been terminated, and noting that the hospital had settled litigation regarding the leaked records.

The current lawsuit addresses Schefter's and ESPN's legal obligations after Schefter received the records. Pierre-Paul claims that Schefter's tweet violated § 456.057(11) of the statute, which provides that, if medical records are disclosed to a third party, that third party "is prohibited from further disclosing any information in the medical record without the expressed written consent of the patient or the patient's legal representative."

It remains to be seen whether Pierre-Paul can successfully convince the court that Schefter should be held responsible for further distributing medical records that hospital employees should never have released. But, for the time being, this remains a cautionary tale about how to handle private and sensitive information when it lands in your lap.

— Kendra L. Berardi

Proportionality Makes a Comeback

After seemingly endless years of rulemaking, the first decisions applying the amended Federal Rules of Civil Procedure have begun to trickle out. Not surprisingly, there have been no game changers to date, but early signs point to a heavy emphasis on the principles of proportionality, a concept entrenched in the Rules since the 1980s but given new life with the amendments to Rule 26.

Indeed, in January alone, federal district courts in New York, California, and Georgia all looked to the proportionality principles contained in Rule 26(b)(1) in deciding discovery disputes.

In *Henry v. Morgan Hotel Group*, 2016 WL 303114 (S.D.N.Y. Jan. 25, 2016), the court concluded that a third-party subpoena was improper, in part, because it failed to apply amended Rule 26(b)(1), which emphasizes "the need to analyze proportionality before ordering production of relevant information." Similarly, in California, the court in *ChriMar Systems v. Cisco Systems*, 2016 WL 126556 (N.D. Cal. Jan. 12, 2016), credited the producing party's objection that a request was disproportionate where it sought "information from anywhere in the world without any temporal limitation." Finally, a Georgia court granted a motion to compel, awarded attorneys' fees, and ordered counsel to familiarize themselves with the amendments, noting that the amendments "elevate [...] the proportionality factors previous found in Rule 26(b)(2)(c)." *See Herrera v. Planation Sweets*, 2016 WL 183058 (S.D. Ga. Jan. 14, 2016).

While it will likely take several years for the full impact of the amendments to be felt in the case law, litigants beware—proportionality is back and the courts are taking notice.

— Andrea Donovan Napp

DATA BREACH

University of California Berkeley Breached…Again…Financial Data of 80,000

We previously reported that University of California Berkeley had suffered a data breach affecting 550 students and their families in April 2015. Last Thursday, UC Berkeley announced that a hacker broke into its financial system in December 2015 while it was patching a security issue with its financial management system.

According to UC Berkeley, the hacker had access to the financial data of 80,000 students, alumni, current and former employees, and vendors whose financial information was in the system, including Social Security numbers and bank information.

UC Berkeley is offering one year of free credit monitoring and identity theft insurance for the affected individuals.

— Linn Foster Freedman

LA Department of Health Hit with Ransomware

Days after hackers held Hollywood Presbyterian's health information hostage (view related post), the Los Angeles County Health Department was hit with a ransomware attack that reportedly affected five computers. According to the Health Department, the ransomware did not spread or compromise the department's network.

No ransom was paid in this case. How did it happen? The usual way—employees opened attachments they received via email and in came the malware.

We are seeing more and more sophisticated phishing and spear phishing attacks and more employees being duped by them. This case provides another reason to consider enterprise-wide training of employees so they can detect and prevent a cyber-attack.

— Linn Foster Freedman

New Ponemon Report Says Health Care Organizations Getting Hit by Cyber-Attacks Monthly

Confirming what we are seeing in the field, the Ponemon Institute recently released a new report of a poll of 535 health care IT and IT security professionals that sets forth a dismal state of affairs around data security and intrusions in health care organizations.

The report states that 48 percent of the IT professionals that responded to the survey indicated that their organization had suffered a breach involving patient information in the last year. Further, only 33 percent of those responding rated their organizations' cybersecurity measures as very effective.

The research concludes that health care organizations are hit by a cyber-attack almost once a month, and the IT professionals do not have the resources necessary to adequately secure the systems and data. The respondents stated that, due to a lack of resources, it is difficult to maintain effective strategies around data security. The most common security incident cited by the IT practitioners was exploits of

existing software vulnerabilities and web-borne malware attacks.

The Ponemon Institute also recently issued a report on the cost of breaches caused by mobile devices. Both reports are worth the read and, as always, very well done.

— Linn Foster Freedman

TELEHEALTH

Florida Board of Medicine Allows Prescribing Controlled Substances through Telemedicine for Psychiatric Treatment

The Florida Board of Medicine has changed its Standards for Telemedicine Practice by allowing controlled substances to be prescribed through the use of telemedicine only for the treatment of psychiatric disorders.

Following a pilot program where three psychiatric mental health organizations were given a waiver by the board in order to prescribe controlled substances via telemedicine, the pilot was deemed a success, paving the way for the change in the regulations to allow for prescribing controlled substances only for psychiatric disorders.

The move is being hailed by patient advocates, as it will increase access to treatment for patients with psychiatric disorders. The change in the regulations is consistent with similar provisions in New Hampshire and Delaware.

— Linn Foster Freedman

CYBERSECURITY

Federal Energy Regulatory Commission Issues Final Rule on Cybersecurity Standards

Last month, the Federal Energy Regulatory Commission issued a final rule, which creates standards for cybersecurity of the electric grid.

The final rule adopts seven revised critical infrastructure protection Reliability Standards originally proposed in July 2015.

The revised standards are effective on July 1, 2016, and include:

- Security Management Controls
- Personnel and Training
- Physical Security of BES Cyber Systems
- Systems Security Management

- Recovery Plans for BES Cyber Systems
- Configuration Change Management and Vulnerability Assessments
- Information Protection

The Commission also issued a report that contains recommendations for cyber-incident response and recovery.

— Linn Foster Freedman

IRS-Approved Tax Preparers Fail to Protect Consumers' Privacy, and IRS Increases the Number of Individuals Affected by Filing of Fraudulent Tax Returns

In a report of an audit of 13 IRS-approved tax filing firms, Online Trust Alliance found that 6 of the 13 firms do not provide adequate security against cyber intrusions.

The firms, all members of the IRS's Free File Alliance, provide free tax preparation and e-filing of approximately 100 million federal tax returns. According to Online Trust Alliance, six of the firms are failing to protect consumers' privacy and security when providing the services.

On top of that, the IRS confirmed this week that the initial estimate of those affected by the filing of fraudulent tax returns in 2014 and 2015 as a result of the Get Transcript function—originally estimated at approximately 330,000—is now estimated at 724,000, more than double the original number.

And not to be outdone, KrebsonSecurity wrote this week that the IRS's idea of protecting last year's tax refund victims from fraud against them this year was to provide the victims with an Identity Protection PIN. According to Krebs, the IRS has mailed 2.7 million of these six-digit PINS to prior tax identity theft victims.

But adding insult to the injury, the IRS allows individuals to retrieve their PIN from the IRS website, through the exact same authentication procedures that were used by the identity thieves to file the fraudulent tax returns in the first place. Apparently, the thieves are able to use the same method to retrieve the PIN, file a false tax return, and get the refund from the taxpayer for a second year in a row. The old adage of "death and taxes" should be changed to "death, identity theft, and taxes."

— Linn Foster Freedman

DRONES

FAA Set to Issue a New Rule Specifically for Microdrones

As if the Federal Aviation Administration (FAA) wasn't getting enough flak for its recent drone regulations, it is now considering a separate rule for "microdrones." Microdrones are those drones weighing less than 4.4 pounds and are made of "frangible materials," meaning that these drones would break on impact and, in effect, pose less of a safety threat.

The FAA's Aviation Rulemaking Committee will have until April 1 to "pursue a flexible, performance-

based regulatory framework that addresses potential hazards." Additionally, by April 1, 2016, the committee will issue a final report regarding the operation of microdrones over individuals not participating in their operation and underneath a "covered structure." The Department of Transportation (DOT) secretary said, "We recognize the significant industry interest in expanding commercial access to the National Airspace System. The short deadline [for the committee] reinforces our commitment to a flexible regulatory approach that can accommodate innovation while maintaining today's high levels of safety." We will keep you posted.

— Kathryn M. Rattigan

PRIVACY TIP #24

IRS Issues Alert to Payroll and HR Professionals about Phishing Scheme for W-2s

This week's tip is for businesses and, in particular, the human resources, benefits, and finance departments of all businesses. It doesn't matter what industry you are in or where you or located. It doesn't matter if you have 2 employees or 2,000. Just know that you can become the victim of a sophisticated cyber-attack.

It has become such a problem that the Internal Revenue Service issued an alert on March 1, 2016, to payroll and human resource professionals about a phishing scheme that has affected numerous companies.

The way it works is that a phishing email sent to employees working in the HR and/or payroll department looks like it is from the company's CEO. The email is rigged to look like the real one and is hard to detect that any response to the "real" email is rerouted to a hacker's email. The CEO or another company executive asks the HR or payroll employee to send him or her personally identifiable information about employees of the company, including W-2s.

The email is called a "spoofing" email and contains the actual name of the executive. It asks the employee things like "Kindly send me the individual 2015 W-2 (PDF) and earnings summary of all W-2 of our company staff for a quick review" or "Can you send me the updated list of employees with full details (name, Social Security number, date of birth, home address, salary)."

According to the IRS, "[I]f your CEO appears to be emailing you for a list of company employees, check it out before you respond. Everyone has a responsibility to remain diligent about confirming the identity of people requesting personal information about employees."

So perk up HR and payroll folks and get those antennae up to protect your data and your co-workers' data. Be suspicious anytime anyone asks for the Social Security number of any employee, even if it is an executive. Pick up the phone before following the instructions. Your executives will thank you for your vigilance.

You can access the IRS alert here.

— Linn Foster Freedman

For more thoughtful and timely discussions of legal news and perspectives on issues relating to data

privacy and security, subscribe to our *Data Privacy + Security Insider* blog by e-mail or by RSS feed.

We welcome your feedback and ideas on topics you'd like us to cover. We also encourage you to share this *Insider* and the blog with anyone you think would find it useful.

If you have any questions, please reach out to your contact at Robinson+Cole or Linn F. Freedman, chair of our Data Privacy + Security Team.

Boston | Hartford | New York | Providence | Stamford | Albany | Los Angeles | Miami | New London | rc.com

Robinson & Cole LLP