September 17, 2015

Data Privacy + Security Insider

DATA BREACH

79,000 Students' Data Breached by Vendor of Cal State

We End Violence, a third party vendor that provides online sexual assault prevention training to California State (Cal State) students notified Cal State that it experienced a vulnerability in its underlying code that exposed more than 79,000 students' names, campus IDs, addresses, gender, race, ethnicity, age, relationship status and login credentials. No financial information was exposed, according to Cal State.

Both federal and California law requires the training, and this is one of the three vendors it uses to conduct the training for its students. The vendor is notifying the affected students.

Institutions of higher education are increasingly becoming targets and victims of cyber-hacking due to the extensive amount of personal data that they collect and maintain. This incident is another strong message to educational institutions to shore up security measures.

— Linn Foster Freedman

Ashley Madison Data Breach Update

Anonymous users of the almost 40 million users of the Ashley Madison website have filed suit against internet service providers (ISPs) GoDaddy and Amazon alleging that they have been damaged because the ISPs hosted the stolen data and allowed the stolen data to be easily accessible and searchable (view related posts Aug. 27, Aug. 21 and July 23).

The complaint alleges violations of receipt of stolen property, violation of the Computer Fraud and Abuse Act and negligent infliction of emotional distress and claims damages of not less than $3 million.

— Linn Foster Freedman

HIPAA

Crafting a More Realistic Business Associate Agreement

According to a recent survey by KPMG, 80 percent of health care executives report that their information technology systems have been compromised by cyber-attacks. Most healthcare institutions, the survey found, lack sufficient tracking and reporting capabilities and are failing to report and manage threats that are occurring on a daily basis.

Daily threats are the reality today, including incidents such as ping attacks and other broadcast attacks on system firewalls, port scans, unsuccessful log-on attempts and denials of service. As the KPMG report notes, it is imperative that healthcare organizations enhance their tracking and reporting capabilities as a matter of information security. On a more granular level, it is also important for organizations to review the terms of their business associate agreements (BAAs) to understand their obligations vis-à-vis daily attacks. What they are likely to find is that many BAAs in place today do not adequately address the reality of daily attacks. For example, it is not uncommon for a BAA to impose an obligation on the business associate to report every security incident to the covered entity promptly upon discovery. This type of provision is not only impractical in the current security environment but also a hidden liability for many organizations that have not considered their obligations carefully.

Covered entities and business associates alike should re-evaluate the reporting provisions in their BAAs, giving specific consideration to the reality of daily security threats. One helpful approach is to differentiate between “successful” and “unsuccessful” security incidents, allocating threats faced into one bucket or the other and creating tiered reporting obligations depending on the nature of the threat. This approach would reflect a more realistic understanding of the current security environment and would likely enhance HIPAA compliance by compelling organizations to think about security threats in a more practical, constructive manner.

— Christopher J. Librandi

OCR Settlement Reiterates Importance of Proactive Security Rule Compliance

On September 2, 2015, the U.S. Department of Health & Human Services (HHS) announced that Cancer Care Group, P.C. (CCG), a physician practice located in Indiana, agreed to pay $750,000 as part of a settlement to resolve alleged violations of HIPAA’s Security and Privacy Rules.

The HHS Office for Civil Rights (OCR) initiated an investigation in 2012 after CCG self-reported a breach of unsecured electronic protected health information (ePHI) resulting from the theft of a laptop bag from a CCG employee. The laptop bag contained the employee’s computer, as well as unencrypted back-up media containing ePHI of approximately 55,000 individuals, including names, addresses, dates of birth, Social Security numbers, insurance and clinical information. OCR determined that CCG had never performed an enterprise-wide security risk analysis, and did not have any policies for the protection of ePHI on mobile media, both in violation of the Security Rule. OCR further determined that CCG violated the Privacy Rule by impermissibly disclosing the ePHI of approximately 55,000 individuals.

In addition to the $750,000 payment, CCG’s resolution agreement with OCR requires CCG to comply with a three-year corrective action plan (CAP). Under the CAP, CCG must conduct a comprehensive risk analysis, and then implement an organization-wide risk management plan to mitigate security risks and vulnerabilities identified by the risk analysis. CCG must also review and revise its Security Rule policies, procedures and training program. During the term of the CAP, CCG is subject to heightened reporting requirements for violations of its HIPAA policies and procedures, and must submit annual CAP-compliance reports to HHS.

This latest OCR settlement is yet another reminder to health care providers that for all the attention cyber-attacks rightfully attract, such providers face more immediate security vulnerabilities in the form of their employees. HIPAA-compliant policies and procedures – such as mandatory encryption of back-up media accessed by employees – are the best mechanism for mitigating these security vulnerabilities, and health care providers must proactively ensure compliance with HIPAA's fundamental requirements in order to reduce exposure to costly data breaches.

— Conor O. Duffy

ENFORCEMENT + LITIGATION

Advocate Health Class Action Lawsuit Trimmed

Last week, an Illinois judge dismissed with prejudice five of the six claims levied against Advocate Health Care in a consolidated case of ten cases filed against it following the data breach it experienced in July of 2013 when four unencrypted laptops were stolen from its administrative office, exposing the data of four million patients. The only remaining claim is that of negligence for those plaintiffs who claim they suffered identity theft as a result of the data breach.

— Linn Foster Freedman

Lyft and First National Bank Notified of TCPA Violations by FCC

Late last week, Lyft and First National Bank (FNB) were notified by the Federal Communications Commission (FCC) that they had violated the Telephone Consumer Protection Act (TCPA) when they required users to opt in to receiving automated text messages as a condition of using their services. Specifically, Lyft requires users to receive text messages and other marketing communications in order to use the service, and if they try to opt out, it "made it impossible to use Lyft's services" according to the FCC.

Similarly, FNB forces users to receive marketing text messages to participate in its online banking program and its Apple Pay service and does not give users the ability to opt out.

According to the FCC, the TCPA does not allow companies to condition the use of a good or service on consent and "consumers have the right to choose whether they want marketing calls and texts to their cell phones" and the FCC further stated that it "urges any company that unlawfully conditions its service on consent to unwanted marketing calls and texts to act swiftly to changes it policies."

Following the FCC citation, Lyft promptly revised its terms of service and frequently asked questions to provide users' specific instructions on how to unsubscribe from marketing text messages. Lyft denied that it was sending unwanted communications to its users.

Strong message to all companies: review your opt-in consent procedures for TCPA compliance and update your policies accordingly.

— Linn Foster Freedman

Abercrombie & Hollister to Pay Out $10 Million to Settle TCPA Class Action

On September 11, 2015, Abercrombie & Fitch Co. (Abercrombie) and Hollister Co. (Hollister) agreed to settle a class action complaint alleging that the two clothing retailers violated the Telephone Consumer Protection Act (TCPA) by sending unsolicited text messages to customers' cell phones without prior written express consent. Abercrombie and Hollister agreed to pay $10 million to end this action, to over 3.7 million consumers.

The complaint filed back in August 2014 by lead plaintiffs, Anamaria Chimeno-Buzzi and Lakedrick Reed, alleged that they each received several text message advertisements from the two clothing retailers between June 2014 and April 2014, and that neither of them ever provided their cell phone numbers or prior express written consent. Additionally, the complaint alleged that the text message advertisements did not contain any language related to the customers' ability to opt-out of receiving future text messages.

Abercrombie and Hollister have not yet determined the best practicable means of notice to the potential class members, and have requested that the court appoint a class-action administrator to handle that process. Yet again, another lesson in TCPA compliance, always get prior express written consent, and always allow your customers a chance to opt-out.

— Kathryn M. Rattigan

WEEKLY PRIVACY TIP #1

Password Management

I am asked every day how one can protect their information and privacy in this world of daily data breaches, so we are adding a weekly practical tip to assist our readers in managing their information.

This week's tip is on password management. I know they are hard to remember, and you are supposed to have different passwords for different sites, and that makes it more difficult. But it is true. Recent hacks have demonstrated that when hackers obtain passwords through one hack, they are able to get into multiple sites as users use the same passwords across sites, basically rendering them useless.

Here's the tip: instead of using a bunch of numbers and letters and symbols that you can't remember, use a phrase that you can easily remember. Instead of using the popular password "love," use "I love the Tedeschi Trucks band." Instead of a combination of your children's birthdays, use "My children are teenagers." Both are complex enough that they will be difficult to randomly guess or determine through social engineering.

And please, whatever you do, refrain from putting all of your passwords in a folder entitled "passwords." It sounds ludicrous, but it is a common practice! Stay tuned for more tips to come in the following weeks.

— 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

---