November 25, 2015

DATA BREACH

Starwood Hotels Hit With Payment Card Malware Attack

Last Friday (November 20, 2015), Starwood Hotels announced that it was hit with a payment card malware attack affecting 50 of its North American hotels.

The president of Starwood Hotels Americas stated in a letter to customers dated Friday, "Based on the investigation, we discovered that the point of sale systems at certain Starwood Hotels were infected with malware, enabling unauthorized parties to access payment card data of some of our customers. We want you to know that the affected hotels have taken steps to secure customer payment card information, and the malware no longer presents a threat to customers using payment cards at our hotels."

The affected hotels include various Sheraton Hotels, W Hotels, Westin Hotels, The Phoenician, and the St. Regis Bal Harbour Resort.

— Linn Foster Freedman

IRS Says Taxpayers Can't Sue for Data Breach

The Internal Revenue Service recently requested a federal judge in the D.C. Circuit to dismiss a putative class action suit by taxpayers against the IRS for a data breach earlier this year that affected over 330,000 taxpayers. The IRS alleges that the court doesn't have jurisdiction over the claims as the claims are preempted by the IRS Code, which allows taxpayers to seek relief against the IRS for unlawfully disclosing tax information. Further, the IRS claims that it is immune from liability under the doctrine of sovereign immunity.

Finally, the IRS alleged that the taxpayers do not have standing to sue the IRS as they have not alleged an actual injury.

The breach is alleged to have occurred when unauthorized individuals were able to use the IRS's "Get Transcript" service to get copies of tax returns. The information breached included the taxpayers' full tax transcript, demographic information, children's, and spouse's Social Security numbers, W-2s, income, and financial holdings.

The IRS claimed that the Get Transcript service has been taken down so it can't be used against taxpayers in the future.

The IRS has not provided any relief to taxpayers who were victims of filing of fraudulent tax returns, such as fraud resolution or other mitigation, unlike its assistance to those affected by the OPM data breach.

— Linn Foster Freedman

ENFORCEMENT+LITIGATION

LabMD Update

We reported last week (related post) that LabMD was successful in its fight against the FTC in the administrative investigation against it, prompted by a complaint made to the FTC by Tiversa, when LabMD refused to hire Tiversa to repair an alleged vulnerability in its system. The case was subsequently investigated by the House Committee on Oversight and Government Reform.

LabMD filed suit against Tiversa in federal court in Pennsylvania in January, alleging that Tiversa violated RICO. Tiversa filed suit against LabMD in Pennsylvania state court alleging LabMD defamed it. Both cases are still pending.

Late last week, LabMD requested that Tiversa be sanctioned in the federal court case for violating a protective order prohibiting disclosure of the sworn Affidavit of LabMD CEO Mike Daugherty that was presented to the House Committee on Oversight and Government Reform. LabMD alleges that it has "overwhelmingly clear and convincing" evidence that Tiversa CEO Robert Boback violated the protective order by leaking the Affidavit and is seeking sanctions and a contempt order against Tiversa and Boback. Tiversa denies the allegations.

— Linn Foster Freedman

Rogers Media to Pay $200,000 to Settle Alleged Anti-Spam Law Violations

Canada's anti-spam legislation (CASL) first came into effect July 1, 2014, and several companies have failed to follow its requirements. Now, Rogers Media has agreed to pay $200,000 in fines to the Canada Radio-Television and Telecommunications Commission (CRTC) for sending unsolicited email advertisements in violation of the CASL regulations. The alleged violations occurred between July 2014 and July 2015 when Rogers Media sent e-mails to consumers with an "unsubscribe" button that did not work properly. Businesses are required to respond to a consumers "unsubscribe" request within 10 business days under the CASL. While this was the first unsolicited email sent by Rogers Media, CRTC hopes to make it the last.

— Kathryn M. Rattigan

E-DISCOVERY

The Ethical Duty of Competence in 2015

Although the legal field is not a profession known for embracing change, several developments over the

past year have made it clear that even lawyers have an ethical obligation to understand the basics of modern technology. This summer, Massachusetts became the fourteenth state to include an express duty of technological competence in its state ethics rules for legal professionals. Additionally, 2015 saw the publication of guidance from three state bar associations—New York, Florida, and California—which underscore the breadth and importance of the duty of technological competence.

The New York State Bar Association and Florida's Professional Ethics Committee both issued guidance related to social media usage by lawyers. The Commercial and Federal Litigation Section of the New York State Bar Association promulgated Social Media Ethics Guidelines that advise counsel who utilize social media that they have a minimum obligation to understand how various platforms work and what information will be available to whom.

Similarly, the Florida bar opined on the related issue of the ethics of advising clients to change or alter social media accounts, concluding that a lawyer can advise a client to change privacy settings, or even remove information, as long as the information is preserved.

The opinion issued by the State Bar of California Standing Committee on Professional Responsibility is the most far reaching, examining an attorney's obligations concerning e-discovery generally and concluding that the "ethical duty of competence requires an attorney to assess at the outset of each case what electronic discovery issues might arise during the litigation, including the likelihood that e-discovery will or should be sought by the other side." Notably, this assessment must occur on a case-by-case basis because "the duty of competence may require a higher level of technical knowledge and ability, depending on the e-discovery issues involved in a matter, and the nature of the ESI." Following this analysis, "[a]n attorney lacking the required competence for e-discovery issues has three options: (1) acquire sufficient learning and skill before performance is required; (2) associate with or consult technical consultants or competent counsel; or (3) decline the client representation."

— Andrea Donovan Napp

DATA PRIVACY

FTC Hosts Workshop On Cross-Device Tracking

On November 16, 2015, the Federal Trade Commission (FTC) hosted a workshop focused on the growing practice of cross-device tracking and the associated privacy concerns. While many consumers are aware that their Internet browsing is tracked and used by advertisers, many are unaware they can be monitored across multiple devices while watching television, using mobile applications or wearing fitness trackers. In opening remarks, FTC Chairwoman Edith Ramirez emphasized that companies needed to offer consumers options and safeguards to protect their privacy. Among the privacy concerns discussed were incomprehensible privacy policies and the challenges of opting out of both data tracking and subsequent advertisements. While privacy concerns were paramount, digital advertising representatives emphasized the benefits from cross-device tracking, including improving the user experience by presenting targeted advertisements of interest to the consumer and greater fraud prevention. However, the perceived lack of transparency and effective opt-out mechanisms for consumers clearly has the FTC's attention and will be an issue the agency will continue to monitor and explore.

— Benjamin C. Jensen

CHILDREN'S PRIVACY

Facial Recognition Technology May Be Used As A Method of Verifiable Parental Consent

This week, the Federal Trade Commission (FTC) determined that companies covered by the Children's Online Privacy Protection Act (COPPA) can use facial recognition technologies to match a parent's photo on a government-issued identification to "selfies" that the parent submits via mobile phone or webcam as a method of verifiable parental consent, as required by COPPA. The FTC said, "Evidence demonstrates that a method that involves verifying a government-issued identification and then matching the image on that identification with the captured face of a live person can be 'reasonably calculated, in light of available technology, to ensure that the person providing consent is the child's parent' as required by [COPPA]." Under this new form of verifiable parental consent, the parent would first provide a valid image of their government-issued identification, for example a passport or a driver's license, the authenticity or legitimacy is verified using computer vision technology, algorithms, and image forensics, the parent then is prompted to submit a "selfie" to confirm the photo is of a live person, and finally, the live image is compared to the identification image. This is only the second time the FTC has approved a new verifiable parental consent method since COPPA regulations were revised over two years ago.

— Kathryn M. Rattigan

DRONE PRIVACY

Deck The Halls With…Lots of Drones – Just Don't Forget to Register Them With The FAA

With an estimated 400,000 drones to be sold off the shelves this holiday season, the Federal Aviation Administration (FAA) task force recently released a list of recommendations for recreational drone use, which includes registering each drone with the FAA in a national database. While the FAA already has rules and regulations related to the use of drones for commercial purposes, the FAA is trying now to meet the growing concerns around recreational drone use and the ongoing safety hazards that these recreational drones pose to the public. So, if the FAA follows the task force's recommendations, you will need to register your drone if it weighs anywhere from half a pound to 55 pounds, by submitting your names and addresses to the FAA's national database. The recommendations also suggest at least a $25,000 fine for registration violations—however, that fine would be set in order to deter drug traffickers and tax evaders, but should not apply to users of small recreational drones, the task force said.

But privacy advocates, such as the Electronic Privacy Information Center, say that the FAA needs to require more than just name and address from the drone operator during registration, and should also require information about surveillance capabilities to protect the public from unwanted spying.

The FAA task force that submitted these recommendations was composed of 25 individuals from drone manufacturers to government officials. Now, the FAA will take these recommendations into consideration and then implement a final set of new rules regarding registration. We will keep you updated. Happy drone shopping.

— Kathryn M. Rattigan

PRIVACY TIP #11

Whenever you open a new bank account, credit card, or debit card account or other account such as a health savings account, the bank or credit card company is required to send you a notice of your privacy practices under the Gramm-Leach-Bliley Act.

The notice is usually a separate page in a package that is mailed to you weeks after you open the account. It usually has a chart that lists when the bank or credit card company can “share” your personal information with others for marketing purposes. It gives you a toll free number to call if you want to “opt out” of certain disclosures.

The disclosures you can opt out of are limited, but they include opting out of allowing companies to send all of your personal information, including your Social Security number to other “business partners.” They usually don’t tell you (nor does the law require them to) who those “partners” are. However, these disclosures are often to direct marketing companies that may have access to all of your personal information through a data dump.

As I have said before, I try very hard to limit who has access to my Social Security card. So anytime I receive a Gramm-Leach-Bliley notice in the mail, I call the toll free number and limit the company’s disclosure of my personal information in any way possible. I recommend you do the same as it takes less than a minute, and may prevent your information, including your Social Security number from being disclosed to another entity that can lose it in a data breach.

— 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.
