Attorney Advertising

Robinson+Cole

April 16, 2015

Data Privacy and Security Insider

ENFORCEMENT + LITIGATION

Target Settles with MasterCard for $19M for Data Breach Losses

Target Corp. announced yesterday that it has settled the claims of MasterCard International Inc. (MasterCard) against it to reimburse MasterCard and its card issuers for the losses it sustained in issuing new credit and debit cards to customers following the famous Target data breach in 2013. MasterCard and other financial institutions filed suit against Target for costs related to the data breach, which is pending in federal district court in Minnesota.

The settlement will allow eligible banks and credit unions that issued MasterCard cards to customers following the data breach to make claims for reimbursement for operating costs and fraud-related losses on cards believed to have been affected by the data breach. However, the settlement is conditioned on at least 90% of eligible issuers accepting the offer by May 20. MasterCard is recommending that its financial partners accept the settlement and said that the settlement provides a reasonable resolution to the claims.

Target stated that it will continue to vigorously defend any MasterCard or its issuers claims who do not accept the settlement offer.

— Linn Foster Freedman

FTC Settles with Two Companies Over Misrepresentations of Safe Harbor Compliance

The Federal Trade Commission (FTC) announced last week that it is settling investigations against American International Mailing, Inc. and TES Franchising LLC alleging that each were misrepresenting to consumers that they complied with the U.S.-European Union Safe Harbor Program and the U.S.-Swiss Safe Harbor Program. The Consent Orders are open for comment until May 7, 2015.

The FTC alleges that both companies were not in compliance with the safe harbor programs and that they misrepresented to consumers that they were certified when in fact, their certifications had expired years before the investigation.

Both companies have been presented with proposed Consent Orders by the FTC agreeing not to

misrepresent safe harbor status or certification in “advertising, marketing, promotion, offering for sale, or sale of any product or service, in or affecting commerce” or that they are a member of, adheres or complies with, is certified or participates in any privacy or security program sponsored by a government or self-regulatory or standard setting organization. The companies must also provide the FTC with all advertising and promotional material that make any representations about safe harbor status over the next 5 years. In standard FTC fashion, the Order would be effective for 20 years.

The message is clear: anyone representing to consumers that it complies with safe harbor status or has self-certified to compliance on its website or otherwise, may wish to consider periodically checking that certification is current and that it is reviewed and updated on a yearly basis.

— Linn Foster Freedman

Jury Awards Plaintiff $12,000 for Dish Network’s TCPA Violations

On April 2, 2015, Ohio U.S. Magistrate Judge Stephanie K. Bowman ruled for the plaintiff, Benjamin Maraan, in his Telephone Consumer Protection Act (TCPA) case against Dish Network LLC (Dish). Maraan was awarded $12,000 for Dish’s 22 violations of the TCPA. Dish made these 22 calls to Maraan’s grandson’s cell phone using automated dialing technology without his prior express consent. After only about an hour of deliberations, a jury returned a verdict in favor of Maraan, and recommended that the court award the maximum penalty for each TCPA violation – that is $500 each. Judge Bowman added an additional $1,000 to the jury’s $11,000 statutory damages for phone calls that Dish had made willingly and knowingly.

This brings to close Maraan’s suit filed back in June 2013. Dish purports that it was legitimately trying to contact a customer who had a delinquent bill, and that the calls to Maraan’s grandson were simply a mistake. Businesses that are aware of the stringent TCPA regulations and that properly document customer consent so as not to make calls like this, will be most likely to avoid the high costs of TCPA violations.

— Kathryn M. Sylvia

DATA BREACH

NLRB to Define an Employer’s Duty to a Labor Union Following a Data Breach

In October 2014, the United States Postal Service (USPS) disclosed a cybersecurity data breach affecting approximately 800,000 current and former employees. The USPS later determined that, for some, the breach may have included names, addresses, dates of birth, social security numbers, and even medical records. Like others before it who have experienced this type of data breach, the USPS offered those affected a full year of free credit monitoring. The difference in this case is that many of those impacted included employees represented by labor unions.

Acting on behalf of those employees, the labor unions (the American Postal Workers Union, AFL-CIO, and the National Rural Letter Carriers’ Association) sought information from the USPS about the breach and demanded to bargain with the USPS about the effects of the breach on the union-represented employees. The USPS rejected the Unions’ demand, and, in November of 2014, the Unions filed unfair labor practice charges against the USPS with the National Labor Relations Board (NLRB).

On March 31, 2015, the NLRB found merit in those charges and issued complaints against the USPS alleging that it violated the law by:

- Refusing to bargain with the Unions about the effects of the "cybersecurity breach" on union-represented employees;
- Failing to provide information to the Unions concerning the data breach as it relates to union-represented employees; and
- Unilaterally granting one year of free credit monitoring services and fraud insurance to union-represented employees without first giving the Unions notice and an opportunity to bargain about those benefits.

The NLRB has long-held that an employer must bargain with the union representing its employees before granting a benefit and about issues impacting terms and conditions of employment. As part of the general duty to bargain, employers must also provide those unions with the information they require to represent those employees effectively. Even when faced with confidentiality concerns, the law requires that an employer bargain with unions about those confidentiality issues. How the NLRB will apply these principles to a cybersecurity data breach remains to be seen. For example, at what stage must an employer begin to involve the union and how much information must it share? How much bargaining will it require and what happens in the meantime?

Trials are scheduled before administrative law judges for May of this year. As these cases work their way through the administrative process, we can expect some guidance on the extent to which an employer must involve unions when they experience a cybersecurity breach.

— Natale V. Di Natale

Lufthansa Frequent Flyer Accounts Hacked

Lufthansa confirmed last week that an unknown number of their customers' accounts were hacked and the hackers were able to use illegally obtained usernames and passwords in order to use frequent flyer miles to make purchases. Lufthansa has reimbursed its affected customers. Lufthansa reported that the hackers used botnets to infect computers to log on to customers' accounts on LH.com. This is in the wake of similar incidents reported by other major airlines.

Lufthansa stated that the information the hackers used did not originate from its databases. It is presumed that the information was purchased by the hackers on the black market. It is easy money for hackers as individuals often use the same username and password across different platforms and applications. It is a reminder to all of us to use different usernames and passwords on any account, but particularly financial accounts. We don't often think of frequent flyer miles as a financial account, but miles can be used to purchase air travel and merchandise. So go change your usernames and passwords now.

— Linn Foster Freedman

SOCIAL MEDIA

Employers Beware: Montana and Virginia are the Newest States to Limit Employers' Access to Personal Social Media Accounts Bringing the Total Number of States to 19

On April 8, the Montana legislature sent its new social media law to the Governor for signature and on March 23, Virginia passed legislation prohibiting an employer from requiring, requesting, or causing a current or prospective employee to disclose his or her username and password of social media accounts or requiring an employee to obtain the username and password or other access to a current or prospective employee's social media account. These two states have joined 17 others that contain similar

prohibitions.

Connecticut and West Virginia failed to pass similar social media legislation earlier this month, and Mississippi and Wyoming rejected their proposed legislation in February.

Last year, approximately 28 states considered social media legislation that in general, prohibited employers access to social media accounts, but only 7 states were successful in enacting laws on the subject matter, including Louisiana, Maine (which authorized a study into the issue), New Hampshire, Oklahoma, Rhode Island, Tennessee, and Wisconsin. This brought the total number of states who have enacted such legislation to 17, as 10 states (Arkansas, Colorado, Illinois, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont (authorizing a study), and Washington) enacted social media legislation in 2013.

Employers doing business in these 19 states may wish to review the statutory prohibitions with counsel, and employers in the other states—keep watching social media legislation as your state is probably not far behind. Whether your state prohibits access to social media accounts of your employees or prospective employees through statute or not, this is an area that warrants caution.

— Linn Foster Freedman

NLRB Determines Vulgar Facebook Posts Protected Concerted Activity

The National Labor Relations Board (NLRB) determined that Pier Sixty LLC, a New York catering service, violated federal labor law by firing an employee server after he posted a Facebook message protesting supervisory abuse and encouraging other employees to vote for a union in an upcoming election. At a recent catering event, employee, Hernan Perez, posted profane messages on his Facebook page about the company's assistant banquet director and included "Vote YES for the UNION!!!" at the end of his profanity. After the company investigated the allegations about the posting, they fired Perez about two weeks later. However, the NLRB found that Perez's "impulsive reaction" on Facebook was "activity protected by the [National Labor Relations] Act and his post "reflected his exasperated frustration and stress after months of concertedly protesting disrespectful treatment by managers." The NLRB also determined that Perez's behavior did not interrupt or interfere with the company's customer relations, and while the board states that it does not condone the vulgar language used by Perez in his Facebook post, he never lost the protection of the NLRA and had therefore been unlawfully fired for his protected concerted activity.

— Kathryn M. Sylvia

HEALTH INFORMATION PRIVACY

HHS/Office of the National Coordinator Issues Report that Health Information Sharing is Being Blocked to Gain a Competitive Edge

In a scathing report released last Friday, the Department of Health and Human Services Office of the National Coordinator (ONC) accused hospitals and software vendors of preventing the sharing of health information in order for hospitals to prevent patients from being referred to or seeking treatment at nonaffiliated providers and electronic medical record vendors to try to keep market share from their competitors.

The effect of the "information blocking" has been to "frustrate the goals" of the Health Information Technology for Economic and Clinical Health Act (HITECH) which provided close to $30 billion in financial incentives to hospitals and eligible providers to become meaningful users of certified electronic health record systems (EHR).

According to the report, hospitals are blocking the sharing of health information "to control referrals and enhance their market dominance." There are claims that hospitals are using the Health Insurance Portability and Accountability Act (HIPAA) to prohibit sharing health information even in a treatment setting, when in fact HIPAA allows the exchange of information for treatment, payment, and operations. Further, EHR vendors are blocking information to "lock providers and consumers to rigid technologies and information sharing networks that reinforce the market dominance of established players and prevent competition from more innovative technologies and services…"

The ONC is not happy with the results of the report and indicated that it will take swift and strong action to prevent this behavior from continuing. It stated that it will get more aggressive on approving EMR technology and is considering suspending or terminated vendors with certification if interoperability is frustrated by its technology. It also announced that it would issue a proposed rule requiring transparency and disclosure obligation of EHR vendors. It will also refer cases to the Federal Trade Commission if it is believed that the information blocking is an antitrust violation.

The report is a strong message to hospitals and EHR vendors, who likely will want to evaluate it in the context of a risk management program.

— Linn Foster Freedman

To get more thoughtful and timely discussions of legal news and perspectives on various issues relating to data privacy and security, subscribe to our *Data Privacy and Security Insider* blog. Check it out at www.dataprivacyandsecurityinsider.com and subscribe 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 and Security Team.
