Skadden

PRIVACY & CYBERSECURITY UPDATE

OCTOBER 2014

CONTENTS (click on the titles below to view articles)

LEARN MORE

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on Page 8, or your regular Skadden contact.

OCTOBER: NATIONAL CYBER SECURITY AWARENESS MONTH

October 2014 was the 11th annual National Cyber Security Awareness Month, sponsored by the Department of Homeland Security (DHS) in cooperation with the National Cyber Security Alliance and the Multi-State Information Sharing and Analysis Center. DHS emphasizes that cybersecurity is the shared responsibility of the public sector, the private sector and the general public. In sponsoring the month, the agency and its partners seek to promote awareness of cyber threats to the nation's critical infrastructure and educate citizens about measures they can take to protect themselves from such threats. DHS highlighted its efforts to promote online safety through its ongoing Stop.Think.Connect campaign, which focuses on the importance of securing the increasing number of household devices that connect to the Internet and noted the ways in which various branches of law enforcement are tailoring their efforts to combat cybercrime.

NEW CALIFORNIA DATA PROTECTION LAW

On September 30, galvanized by the many high-profile data breaches suffered during the past year by retailers such as Target, Neiman Marcus and Home Depot, California Governor Jerry Brown signed into law Assembly Bill No. 1710 (the Amendment), which enhances California's existing laws concerning the protection of sensitive personal information.[1] The Amendment, which will take effect on January 1, 2015, seeks to improve the protection of personal information of California residents by making three changes to California's existing laws concerning breach notifications and the protection of personal data:

Broadening the obligation to implement reasonable security procedures to include not only businesses that own or license personal information, but also data brokers, third-party service providers, and other businesses that "maintain" such information without owning or licensing it from others;

Prohibiting the sale of an individual's social security number, except where the release of the social security number is ancillary to a legitimate transaction; and

Enhancing consumer protections in the event of a data breach by requiring "the source of the breach" to "provide appropriate identity theft prevention and mitigation services, if any," at no cost to the affected person for at least one year.

INCREASED SCOPE OF COVERED BUSINESSES

California law currently requires all businesses that "own or license personal information about Californians to provide reasonable security for that information." The Amendment broadens the applicability of the statutory requirement to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access,

[1] A copy of the California law can be found at http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140AB1710.

destruction, use, modification, or disclosure" to include third parties who "maintain" but do not "own or license" personal information of California residents.

PROHIBITING SALE OF SOCIAL SECURITY NUMBERS FOR MARKETING OR OTHER PURPOSES

A provision of the Amendment regulating the handling of social security numbers supplements California law by prohibiting the sale of, advertising the sale of or offering to sell an individual's social security number. The amended law permits the release of a social security number where such release "is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a legitimate business purpose." However, the statute expressly provides that the "[r]elease of an individual's social security number for marketing purposes is not permitted."

POST-BREACH PROVISION OF IDENTITY THEFT PREVENTION AND MITIGATION SERVICES

The Amendment also adds a new obligation regarding the provision of "identity theft prevention and mitigation services." The provision reads:

> If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed [an individual's social security number, driver's license number or California identification card number].

Some commentators have noted that the "if any" language of this provision is ambiguous and could act to narrow the statute. According to these commentators, one could read the provision merely to require that, to the extent identity theft prevention and mitigation is offered, such services must be provided at no cost to the affected person for at least 12 months. Nonetheless, the better reading of the provision, and one that would be consistent with the legislative intent, is that it requires affected persons be provided with identity theft prevention services for at least 12 months at no cost to the affected person, and that if mitigation services are also provided, these must also be for 12 months and at no cost. Assuming this latter interpretation is the correct one, the amended statute will be the first of its kind in the United States to require the provision of such services as a statutorily mandated remedy for certain data breaches.

PRACTICE POINTS

Companies that handle data of California residents should take steps to mitigate the risk of violating California's new data security law, which comes into effect on January 1. These steps should include:

- Reviewing how social security numbers are used by the company;
- Including in the company's periodic review of its privacy and security policies and practices (i) an assessment of the types of personal information that are owned, licensed or otherwise held by the organization, and (ii) what forms of identity theft prevention and mitigation services might be warranted in the event of a breach resulting in unauthorized access to such personal information; and
- Depending on the degree of risk and nature of personal information owned, licensed or otherwise held by the organization (and given that even the most robust security practices can be thwarted by a sufficiently persistent and sophisticated attacker), consider procuring cyber insurance to decrease the overall risk to the company.

Return to Table of Contents

OBAMA SIGNS CYBERSECURITY EXECUTIVE ORDER

On October 17, 2014, President Obama signed an executive order requiring increased security for consumer payments processed by the federal government and calling for several other measures to secure consumer payment information.[2] The executive order is part of the government's new "BuySecure Initiative," which aims to increase security for consumer payment information, including by encouraging (and, in the case of the government agencies subject to the executive order, mandating) the use of chip and PIN technologies in credit, debit and other payment cards.

In a payment card using chip and PIN technology (also known as "EMV" technology after its originators, EuroPay, MasterCard and Visa) the magnetic strip on the card is replaced with a microchip, and consumers are required to provide a PIN when using the card in face-to-face (as opposed to online) transactions. The technology is used widely in the United Kingdom, Canada and Australia, and is credited with significantly reducing in-store credit card fraud in those jurisdictions.

The executive order requires use of chip and PIN technology in credit, debit and other payment cards issued by the executive departments and agencies to government employees, as well as debit cards issued by the government as part of benefits programs. By January 1, 2015, payment cards provided through the General Services Administration and Direct Express prepaid debit cards for government benefits must have chip and PIN technology, and other agencies with payment card programs must provide a plan for implementing chip and PIN technology in their own payment cards.

The executive order also calls for the following measures to help reduce the burden on consumers who have been victims of identity theft:

- Increased reporting of identity theft by federal law enforcement agencies to the National Cyber-Forensics and Training Alliance's Internet Fraud Alert System, which in turn alerts financial institutions and other service providers when a customer's information has been compromised;
- Enhancing (by May 15, 2015) the www.identitytheft.gov website, which is the Federal Trade Commission's resource for consumers who have been victims of identity theft, so that it includes a streamlined process for reporting identify theft to multiple credit bureaus; and

Implementing multifactor authentication and an effective identity proofing process by all agencies making personal data accessible to citizens online.

As part of the BuySecure Initiative, retailers Home Depot, Target, Walgreens and Wal-Mart have agreed to install terminals that accept chip and PIN cards in all of their stores in early 2015. Other private sector initiatives announced along with the executive order include a program by American Express that will assist small businesses in upgrading their point-of-sale terminals, a Visa program designed to educate consumers and merchants on secure payment technologies, and a MasterCard program to provide its customers with identity theft monitoring. In addition, Citi, in partnership with FICO, will make credit scores available on a monthly basis to its consumer card customers to help them detect fraudulent activity early.

President Obama also announced that a Summit on Cybersecurity and Consumer Protection will take place later this year and will focus on additional ways to protect consumer financial data. He again asked Congress to pass legislation that will clarify companies' responsibility to consumers whose payment information has been compromised.

---

[2] A copy of the executive order can be found at http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions.

Return to Table of Contents

FTC CAUTIONS EXECUTIVES ABOUT PERSONAL LIABILITY FOR FALSE ADVERTISING AND PRIVACY VIOLATIONS

In a presentation to the National Advertising Division at the Advertising Self-Regulatory Council's annual conference late last month, a senior attorney from the Federal Trade Commission (FTC) highlighted the fact that corporate executives can be held personally liable for false advertising and privacy violations committed by their businesses. The FTC attorney, Lesley A. Fair from the Division of Consumer Protection and Business Education, emphasized that individuals can be personally liable for violations of the FTC Act even if their actions took place on behalf of an incorporated entity. She pointed to a recent Fourth Circuit case where an executive was held personally liable for $163 million in damages as an example.

In *Federal Trade Commission v. Ross*,[3] Innovative Marketing, Inc., operating under a variety of names, asked consumers to run a free security scan via a pop-up window, and then proceeded to download security software onto the consumer's computer regardless of the answer. This program was so-called "scareware" which alerted consumers that a scan had been run and had found fictitious malware, viruses, or other issues, and then offered consumers the option to purchase software to fix the alleged problem, at a cost of $40 to $60. According to the FTC, over a million consumers were tricked into purchasing the product.

The FTC first received a temporary injunction preventing the company from offering this type of software in 2008. It then brought action against a number of defendants, including Kristy Ross, a vice president at the company. The district court entered summary judgment in favor of the FTC on the issue of whether the advertising was deceptive. The judgment was for joint and several liability for $163 million. Ross was the only defendant to defend against the suit; the others settled or had default judgments entered against them. This left Ross, as the only remaining defendant, personally liable for the full $163 million.

Ross appealed the decision on several grounds, including that the FTC lacked the requisite authority to seek monetary judgments under the FTC Act, and that the court had applied the wrongly formulated mental state requirement. In February 2014, the Fourth Circuit found in favor of the FTC. With regard to the FTC's ability to seek monetary judgments, the court held that under the FTC Act, Congress authorized the district court to exercise the full measure of its equitable jurisdiction in order to issue "complete relief," which would include monetary consumer redress, a form of equitable relief. The Fourth Circuit stated that to rule otherwise would "forsake almost thirty years of federal appellate decisions and create a circuit split."

Ross also appealed on the grounds that the district court had applied the wrong standard for the mental state required in order to hold an individual personally liable under the FTC Act. The district court had stated that an individual could be held individually liable if he or she participated directly in the deceptive practices or had the authority to control them, coupled with knowledge of the deceptive conduct. The knowledge requirement could be satisfied by demonstrating actual knowledge, reckless indifference to the truth, or willful blindness. Ross proposed a standard from securities fraud jurisprudence that would have required the FTC to demonstrate actual awareness of specific deceptive practices. The court rejected this standard, citing the unfairness of holding "the lifeless entity of a corporation" liable, while sparing the individuals who actually perpetrated the fraud. Instead, the court held that one may be individually liable under the FTC Act where he or she (i) participated directly in the deceptive practices or had the authority to control such practices, and (ii) had or should have had knowledge of the deceptive practices.

Although this case was a particularly egregious example of a company operating a scam designed specifically to deceive the public, it serves as a reminder that executives may be held personally liable for deceiving customers under the FTC Act. Ms. Fair's statements at

[3] A copy of the Fourth Circuit's decision can be found at http://www.ca4.uscourts.gov/Opinions/Published/122340.P.pdf.

a recent privacy conference suggests that the FTC may not hesitate to exercise its authority against executives whose companies are engaged in dubious privacy practices. FTC authority is not limited to egregious cases, but can be applied wherever corporations are engaging in deceptive practices. In these circumstances, individual executives, like Kristy Ross, may be held personally liable for large damage awards.

Return to Table of Contents

FCC ENTERS THE DATA PRIVACY ENFORCEMENT ARENA

Although companies typically view the FTC and state attorneys general as the primary enforcers of data security lapses, entities under the purview of the Federal Communications Commission (FCC) may now have that agency to contend with as well.

On October 24, 2014, the FCC issued a Notice Of Apparent Liability For Forfeiture in the matter of TerraCom, Inc. and YourTel America, two common carriers providing telecommunications

Services to low-income households. According to the FCC, the two companies collected personal information such as names, addresses, Social Security numbers and driver's licenses from low-income individuals and "stored them on unprotected Internet servers that anyone in the world could access with a search engine and basic manipulation." Apparently, the information was stored in two publicly accessible folders on the Internet that did not include password protection or encryption. The companies' actions were first revealed by an investigative reporter working for Scripps Howard News Service who was able to access over 100,000 consumer records on the companies' websites by using simple Google searches. The companies initially alleged that Scripps had engaged in hacking activities.

The FCC's charge against the two companies reads very much like certain FTC actions that have been brought in the last two years. Specifically, the FCC alleged that the companies:

- failed to properly protect the confidentiality of consumers' personal information;
- failed to employ reasonable data security practices to protect consumers' personal information;
- engaged in deceptive and misleading practices by representing to consumers in the companies' privacy policies that they employed appropriate technologies to protect consumers' personal information when, in fact, they had not; and
- engaged in unjust and unreasonable practices by not fully informing consumers that their personal information had been compromised by third-party access.

The FCC concluded that these actions violated Sections 201(b) and 222(a) of the Communications Act of 1934, and proposed a forfeiture of $10 million. Section 222(a) imposes a duty on every telecommunications carrier "to protect the confidentiality of proprietary information of, and relating to, ... customers." Section 201(b) of the Act states, in pertinent part, that "[a]ll charges, practices, classifications, and regulations for and in connection with [interstate or foreign] communication service [by wire or radio], shall be just and reasonable, and any such charge, practice, classification, or regulation that is unjust or unreasonable is declared to be unlawful."

Companies under the FCC's jurisdiction should be mindful of how they protect consumer information, and like all companies today, careful about the representations they make regarding the level of security they provide to consumers.

Return to Table of Contents

CFPB FINALIZES RULE REGARDING PRIVACY NOTICES UNDER GRAMM-LEACH-BLILEY

The Consumer Financial Protection Bureau (CFPB) finalized a new rule in October that allows financial institutions to deliver privacy notices to customers by posting them online.[4] Financial institutions are currently required under the Gramm-Leach Bliley Act to send hard copies of privacy notices on an annual basis to customers. These privacy notices describe whether and how a financial institution shares its customers' nonpublic personal information with unaffiliated third parties and informs customers of their right to opt out of this practice. The CFPB estimates that use of the online delivery method, which allows financial institutions to avoid physically mailing separate notices to customers, could save the financial services industry approximately $17 million annually.

A financial institution may only use the online delivery method if (i) the financial institution does not share customer data in a way that would trigger a customer's opt-out rights and (ii) the information included in its privacy notice has not changed since the customer received the prior notice. The CFPB suggests that the new rule encourages financial institutions to limit data sharing in an effort to reduce the costs associated with delivering hard copies of privacy notices. The rule also allows customers to have easy access to the privacy notice, rather than having to locate a single paper copy that they likely discarded.

In order to use the online delivery method, the financial institution must use a model disclosure form developed by regulators and notify customers at least once annually through another regular consumer communication, such as a monthly bill or coupon book, that its annual privacy notice is available online (and in paper by request). The institution must post the annual privacy notice in "clear and conspicuous manner on a page of its website, without requiring a login or similar step or agreement to any conditions to access the notice." The rule will become effective immediately after its publication in the Federal Register.

Return to Table of Contents

NEW YORK DEPARTMENT OF FINANCIAL SERVICES REQUESTS VENDOR CYBERSECURITY INFORMATION FROM BANKS

On October 21, 2014, the superintendent of New York's Department of Financial Services, Benjamin Lawsky, sent a letter to dozens of banks regarding cybersecurity risks arising out of the use of third-party service providers. The letter asks banks to describe their due diligence processes used to evaluate the adequacy of their third-party service providers' cybersecurity controls, and how data shared by the banks with such third-party service providers is safeguarded. Lawsky states in the letter that "it is abundantly clear that, in many respects, a firm's level of cybersecurity is only as good as the cybersecurity of its vendors," and that "it is important that financial institutions are able to identify, monitor and mitigate any cybersecurity risks posed by their third-party vendor relationships, including but not limited to law firms and accounting firms."

According to the letter, the Department of Financial Services is in the process of reviewing how banks manage the cybersecurity aspects of their relationships with third-party vendors, and is considering introducing a requirement that financial institutions obtain representations and warranties from third-party service providers regarding their cybersecurity standards. As part of this review process, Lawsky has requested that the banks respond by November 4: (i) describing the due diligence processes used to evaluate the cybersecurity practices of their third-party service providers, (ii) providing copies of related policies and procedures, and (iii) detailing protections used to safeguard sensitive data shared with third-party service providers. The letter also requests that the banks identify any steps they have taken to comply with the relevant portions of the voluntary cybersecurity framework of the National Institute of Standards and Technology, issued in February of this year, and to list any protections against

[4] A copy of the rule can be found at http://files.consumerfinance.gov/f/201410_cfpb_final-rule_annual-privacy-notice.pdf.

loss, including relevant insurance coverage, incurred as a result of an information security failure by a third-party service provider.

Return to Table of Contents

LAWS REGULATE ACCESS TO DIGITAL ACCOUNTS ON A USER'S DEATH

An increasing number of states have begun implementing legislation that addresses the administration of an individual's digital assets, such as email accounts, social media accounts and cloud storage data, upon the death of the individual. In August, Delaware passed the most expansive legislation to date, which grants an executor of the decedent's will access to the digital accounts of the decedent.[5] Access does not extend to friends and family of the decedent, but the executor has the discretion to transfer the account information to a friend or family member of the decedent.

The Delaware legislation was modeled after the Uniform Fiduciary Access to Digital Assets Act (the UFADAA), approved in July 2014 by the Uniform Law Commission, a group appointed by state governments to draft and lobby for new state laws.[6] The UFADAA's purpose is to grant fiduciaries authority to "access, control, or copy digital assets and accounts." In the context of the UFADAA, a fiduciary refers to an executor, administrator or personal representative of an estate as well as a guardian, trustee or agent.

Approximately 10 states have considered various versions of the recently passed Delaware legislation and a number of others have already passed legislation addressing this issue. A Connecticut statute, for example, authorizes a fiduciary to access a deceased individual's email accounts (but does not specifically address other digital accounts).[7] Rhode Island has enacted a statute that requires fiduciaries to obtain a court order before accessing digital accounts of the deceased.[8] Virginia has passed a law that gives a deceased minor child's personal representatives, who almost always are the child's parents, access to the child's digital accounts.[9] New York currently is considering legislation governing fiduciaries' access to the digital assets and accounts of deceased individuals.

Such laws have raised privacy concerns from companies who host these digital accounts. In particular, the State Privacy and Security Coalition, a trade association representing 20 such companies, including Google, Facebook and Yahoo!, believes that allowing access to these accounts violates the privacy of the deceased individual as well as that of still-living third parties who had communicated with the deceased. The Coalition pointed out that the law could, for example, expose to the executor the particularly confidential communications of patients with deceased doctors, psychiatrists and clergy.

Further, critics of the UFADAA and similar state laws point out that compliance with state laws based on the UFADAA could constitute a violation of federal law. The Electronic Communications Privacy Act of 1986 (the ECPA) prohibits an electronic communications service from knowingly divulging the contents of a communication stored or maintained on that service unless the disclosure is made "to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient of such communication."[10] There is no exception for disclosure to fiduciaries. While some of the state laws expressly state that the personal information should not be disclosed if such disclosure would violate federal law,

---

[5] A copy of the Delaware law can be found at http://www.legis.delaware.gov/LIS/lis147.nsf/vwLegislation/HB+345/$file/legis.html?open.
[6] A copy of the UFADAA can be found at http://www.uniformlaws.org/Act.aspx?title=Fiduciary%20Access%20to%20Digital%20Assets.
[7] A copy of the Connecticut law can be found at http://www.cga.ct.gov/2005/act/Pa/2005PA-00136-R00SB-00262-PA.htm.
[8] A copy of the Rhode Island law can be found at http://webserver.rilin.state.ri.us/Statutes/TITLE33/33-27/33-27-3.HTM.
[9] A copy of the Virginia law can be found at http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+64.2-110.
[10] A copy of the Electronic Communications Privacy Act can be found at http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.

this still requires companies to conduct the legal analysis and make a judgment call prior to disclosure. Companies must also comply with applicable state privacy laws, which may require notification to individuals and governmental agencies when certain personal information, such as health information, is disclosed without the authorization of the individual to whom the information relates.

The Coalition also has noted that the Delaware law disregards service providers' policies and terms of service that might prohibit such companies from granting an executor access to the digital account of a deceased person. Indeed, some certain terms of use contain specific provisions addressing the disposition of a user's account in the event of the user's death. For example, Google allows a user to designate an assignee of his or her account to a beneficiary in the event of his or her death. Twitter permits an executor or a verified family member to deactivate a deceased individual's account if a death certificate and a government-issued form of identification is provided. If provisions like these conflict with applicable state law, a company could be faced with a choice between complying with law and complying with their own terms of use.

Companies offering electronic communications services should, at a minimum, make sure that their terms of use allow them to comply with the law in the event that a law conflicts with the terms. Such companies also may want to revisit broad statements about how they address access to data upon the death of a user.

Return to Table of Contents

SKADDEN CONTACTS

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
Four Times Square
New York, NY 10036
212.735.3000