September 2015 A publication of the Data Breach, Cybersecurity and Privacy Team

The Arnold & Porter Data Security Roundup reports on recent legal developments in the realms of data security, data breach, data privacy, and cybersecurity. For more information on Arnold & Porter's related areas, please visit our Data Breach, Cybersecurity, and Privacy practices.

IN-HOUSE COUNSEL TIP

If you are a government contractor, ensure that you are aware of all regulatory as well as contractual privacy requirements, and maintain required written documentation to demonstrate compliance.

Executive and Regulatory Developments

Third Circuit Rules That FTC Has Authority to Regulate Cybersecurity

On August 24, 2015, the Third Circuit held that the Federal Trade Commission (FTC) could move forward with its enforcement actions against Wyndham Worldwide Corporation, a hospitality company that experienced three cybersecurity attacks in 2008 and 2009 resulting in the disclosure of confidential payment information for over 619,000 consumers and at least US$10.6 million in fraud loss. The court held that the FTC has authority to regulate cybersecurity under Section 45(a) of the FTC Act, which prohibits "unfair or deceptive acts or practices in or affecting commerce." The court further held that Wyndham had fair notice that its specific cybersecurity practices could fall short of Section 45(a), rejecting Wyndham's claim that it was entitled to notice of the *specific* cybersecurity practices required by that statute. In discussing why Wyndham had proper notice that its practices could be inadequate, the court in part cited both a 2007 FTC guidebook that contained a checklist of practices that form a "sound data security plan" and the FTC's history of filing complaints and entering consent decrees in administrative cases raising unfairness claims based on inadequate corporate cybersecurity. For further information and analysis, see Arnold & Porter's Client Advisory *Court of Appeals Allows FTC's Cyber Security Breach Case Against Wyndham to Proceed* (Aug. 27, 2015).

Defense Contractors Now Subject To New Cybersecurity Regulations

On August 26, 2015, the Department of Defense put into effect an interim rule that expands cybersecurity regulations governing defense contractor information systems that store, process, or transmit "covered defense information" (CDI) in connection with a defense contract. The definition for CDI now encompasses a broader category of data than "unclassified controlled technical information," the term used in prior regulations. Among other things, the interim rule requires that all defense contractors provide "adequate security" for CDI. Defense contractors must also fully investigate and report any cyber incidents affecting contractor information systems with CDI. For further information and analysis by Arnold & Porter, see *'Adequate Security' and Full Disclosure: The DOD's New Cyber Rules for Contractors* (Bloomberg BNA Federal Contracts Report, Sept. 22, 2015).

White House Proposes New Cybersecurity Guidelines For Government Contractors

In early August, the Office of Management and Budget (OMB) released proposed guidance aimed at strengthening cybersecurity protections for "controlled unclassified information" (CUI) on information systems operated by government contractors and subcontractors. The guidelines aim to mitigate the threat of high-profile cyberattacks on government networks by imposing standardized cybersecurity requirements, allowing government access to contractor information systems, and requiring contractors and subcontractors to report "cyber incidents" to federal authorities. Following their release, the proposed guidelines were subject to a 30-day public comment period, which ended on September 10, 2015. The OMB anticipates that the final guidance will be published later this fall. For further information and analysis, see Arnold & Porter Client Advisory *Enhanced Cybersecurity Monitoring and Reporting Obligations for Federal Contractors* (Aug. 20, 2015).

Congressional Research Service Issues Reports on Cyber Intrusion into US Office of Personnel Management and the EMV Chip Card Transition

On July 17, 2015, the CRS issued a report providing an overview of the recent OPM breaches. The report discusses the alleged source of the breaches, potential uses of the stolen information, national security ramifications, and the implications of the breach for the cybersecurity of federal information systems. On September 8, 2015, the CRS also issued a report on the EMV Chip Card Transition (EMV cards are named for the coalition of Europay, MasterCard, and Visa that developed the specifications for the system). The report describes the financial harm and causes of data breaches, the effect of the EMV transition in certain foreign countries, outstanding issues concerning the transition in the United States, and areas of potential congressional interest. October 1, 2015, is the industry imposed deadline for transitioning to chip cards, which provide greater security than the old magnetic stripe cards, and after that date the liability for fraudulent transactions as between the card issuer and the merchant will shift to the merchant if the merchant has not switched to this technology.

SEC Settles Enforcement Action Arising Out of Data Breach

On September 22, 2015, the SEC announced the settlement of a first-of-its-kind enforcement action involving a data security breach at R.T. Jones Capital Equities Management, a St. Louis-based investment adviser. In July 2013, R.T. Jones' web server was hacked, compromising the Personally Identifiable Information (PII) of approximately 100,000 individuals. The action arose out of the company's alleged failure to adopt written policies and procedures to ensure the security and confidentiality of PII, as required by Rule 30(a) of Regulation S-P under the Securities Act of 1933. The SEC charged that R.T. Jones failed to conduct periodic risk assessments, implement a firewall, encrypt PII stored on its server, or maintain a response plan for cybersecurity incidents. Commenting on the case, an SEC official noted that it is important for firms "to have clear procedures in place rather than waiting to react once a breach occurs." The SEC's order ultimately found that R.T. Jones had violated Rule 30(a). Without admitting any wrongdoing, R.T. Jones agreed to cease and desist from committing or causing any future violations of Rule 30(a), to be censured, and to pay a US$75,000 penalty. As of September 22, R.T. Jones had not received any indication that a client suffered financial harm as a result of the data theft. The SEC's press release on the action can be found here.

Industry Developments

National Futures Association Proposes New Information Security Rules For Member Organizations

In August, the board of the National Futures Association (NFA), a self-regulatory organization for the American derivatives industry, approved new rules for its member firms and requested approval of those rules from the Commodity Futures Trading Commission. The NFA abjured a one-size-fits-all approach, instead prescribing a general framework for each member to tailor to its specific risks. The NFA now requires each member to have a formal written information systems security program, approved at the member's executive level. The program should contain: a risk analysis, a description of the safeguards deployed, and the process for evaluating the nature of a security breach. The full text of the proposed rules can be found on the NFA's website.

International Developments

South Korea Stiffens Penalties For Data Security Breaches

South Korea enacted its first comprehensive data security act, the Personal Information Protection Act (PIPA), in 2011. PIPA established rules for the collection, processing, transfer, and protection of personal information, as well as post-breach notification procedures. The original act authorized fines and even

imprisonment for violations of PIPA. In July 2015, the legislature amended PIPA to authorize both statutory (up to three million Korean won) and punitive damages in private actions. The amendments are expected to take effect next year.

Litigation Developments

Financial Institutions Obtain Class Certification in Target Data Breach Litigation; Target Reaches Agreement With Visa and Certain Visa Card Issuers Over Data Breach Losses

On September 16, 2015, the District Court of Minnesota granted certification of a class of entities that had issued payment cards that were compromised in the breach of Target's computer network during the 2013 holiday shopping season. The certification order was issued in the financial institutions "track" of the litigation; Target previously reached a settlement in the consumer track of the litigation, which is pending final approval. In granting class certification, the court noted that the cost to card-issuing entities to replace payment cards was "borne at the time of the breach" and was therefore distinguishable from the future harm alleged in the consumer track of the litigation. The court also ruled that plaintiffs' expert had sufficiently demonstrated that it would be possible to prove classwide common injury and to compute classwide damages, but noted that if classwide damages became unworkable, a damages class could be decertified after the liability phase concludes. Separately, in mid-August, Target announced that it had reached a settlement with Visa and certain Visa card issuers as part of Visa's assessment process. As part of that settlement, Target agreed to pay expenses that the financial institutions incurred during the breach, including costs to reissue cards, up to approximately US$67 million.

State Roundup

California recently released the Statewide Health Information Policy Manual (SHIPM) to provide state departments and entities with guidance on how to comply with state and federal health information laws, including those dealing with privacy, security, and patients' rights. The manual, developed by the California Office of Health Information Integrity (CalOHII)—an office within the California Health and Human Services Agency—is a compendium that offers a uniform interpretation of the governing health information laws and establishes standards and requirements designed to ensure compliance with those laws. Among the federal laws addressed in the SHIPM are the Health Insurance Portability and Accountability Act, the Patients Access to Health Records Act, and the Genetic Information Nondiscrimination Act. The manual also provides guidance under California's Confidentiality of Medical Information Act, Information Practices Act, Lanterman-Petris-Short Act, and Lanterman Developmental Disabilities Act, as well as various applicable provisions of the California Penal Code and the California Health and

Safety Code. Finally, the SHIPM incorporates standards adopted by the National Institute of Standards and Technology and in the California State Administrative Manual. CalOHII has indicated that SHIPM is to be a “living document” that will be updated regularly to account for changes in state or federal law. The full text of the Statewide Health Information Policy Manual, as well as all relevant attachments, are available here.

To receive Arnold & Porter advisories and news on related topics, please click here .

For further information about Arnold & Porter's Data Breach, Privacy and Cybersecurity practices, please contact one of the Data Security team members here.

Your Data Security Roundup Editors:

Marcus A. Asner | Angel Tang Nakamura | Allyson Himelfarb

Kenneth L. Chernof | Nancy L. Perkins | Julie A. Kent

Ronald D. Lee | Emilia P.E. Morris | Brad P. Abel

Sharon D. Mayo