May 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

Ensure that your employee training manuals or other materials are regularly updated to keep your workforce educated on the most effective ways to protect Personally Identifiable Information, Personal Health Information, or other confidential information and to identify potential risks to its protection. Having current and complete documentation can also help strengthen your legal positions with regulators and courts.

New Attorney General Notes Cybersecurity Among Highest Priorities

On April 29, 2015, Attorney General Loretta Lynch spoke at the inaugural meeting of the Department of Justice Criminal Division's Cybersecurity Industry Roundtable. She emphasized that "cybersecurity must be among the highest priorities" for DOJ because of the impact cyber attacks can have on both the national economy and national security. Attorney General Lynch also stressed the need for cooperation across law enforcement, including with the FBI and Secret Service, and between law enforcement and private companies. Her full remarks are available here.

DOJ Releases Cyber Incident Best Practices

Also in April, the Cybersecurity Unit of the Computer Crime & Intellectual Property Section of DOJ's Criminal Division released its first report on "Best Practices for Victim Response and Reporting of Cyber Incidents." The report, which is aimed primarily at smaller organizations with fewer resources, compiles lessons learned by federal prosecutors and provides input from private sector companies that have managed cyber incidents. It contains detailed steps to take before, during, and after a cyber attack, as well as a "preparedness checklist." The Cybersecurity Unit recommends that organizations identify their most important or sensitive information, create an actionable plan, and engage with their legal counsel, law enforcement, and cyber information sharing organizations before a breach occurs. If an attack does happen, the victim should make an initial assessment, attempt to minimize ongoing damage, record information on the attack, and notify personnel within the organization as well as law enforcement, the Department of Homeland Security, and other potential victims. After an incident, the victim should continue monitoring its network and conduct a review of its incident response plan and execution. The full text of the report is available here. For further information and analysis, see Arnold & Porter Client Advisory DOJ Seeks Cybersecurity Cooperation as Best Practice in Responding to Cyber Incidents (May 2015).

Verizon Releases 2015 Data Breach Report

In April, Verizon Enterprise Solutions (a division of Verizon Communications) released its annual Data Breach Investigations Report, which analyzes a year's worth of data security statistics and

observations and offers practical tips to improve information security. Verizon reports that "phishing" campaigns continue to plague secured networks, accounting for approximately 20% of recorded data breach events. According to the report, 23% of recipients open phishing e-mail messages, and 11% click on attachments to those messages. Instances of so-called "RAM scraping," whereby malware intercepts credit card information by accessing the memory of a cash register or credit card terminal during the course of a sales transaction, have also increased. On the other hand, despite known vulnerabilities of mobile devices, mobile malware appears to pose a negligible threat to data security, as only 0.03% of mobile devices were found to be infected with malicious malware. The report also includes industry-by-industry data breach profiles and an analysis of the nine incident classification patterns that appear in 96% of all data attacks. Lastly, a new segment in the report addresses the cost of breaches and provides insight as to how businesses can quantify risk. For example, the estimated loss for a breach affecting 1,000 data records is between $52K and $87K, and the estimated loss for a breach of 10 million records is between $2.1M and $5.2M. The 2015 report concludes with a list of recommended security controls that businesses can implement to reduce their exposure to data breaches, including patching web services, locking out users after multiple failed login attempts, and filtering mail attachments. Access to the full report is available here.

Supreme Court Grants Cert in *Spokeo*

In a move which many were watching, the United States Supreme Court decided on April 27 to grant certiorari in *Spokeo, Inc. v. Robins*, No. 13-1339, which will help clarify the constitutional standing requirements for bringing an action under the Fair Credit Reporting Act. The case, which directly affects online privacy lawsuits and also has significant implications for data breach suits, will likely be set for oral argument in the fall. For more information about the Ninth Circuit opinion giving rise to the Supreme Court petition for certiorari, please refer to the April 2015 issue of the Data Security Roundup, available here.

E.D. La. Dismisses Data Breach Action for Lack of Standing

On May 4, 2015, a federal judge in the Eastern District of Louisiana dismissed a putative class action against eBay stemming from a breach the company experienced in 2014. In that breach, hackers accessed customers' names, encrypted passwords, dates of birth, and contact information, but no financial data or social security numbers. In *Green v. eBay Inc*., No. 14-1688, 2015 WL 2066531 (E.D. La. May 4, 2015), the plaintiff did not allege that any of the information accessed was actually misused or that there was any attempt to use it, so his primary theory of injury was based on an increased risk of identity theft. The court concluded "the mere fact that Plaintiff's information was accessed during the Data Breach is insufficient to establish injury-in-fact," and "the potential threat of identity theft or identity fraud, to the extent any exists in this case, does not confer standing on Plaintiff to pursue this action in federal court." The court noted that its disposition was in line with the vast majority of post-*Clapper* data breach cases to have considered the issue.

State Roundup

Washington amended its data breach notification law to impose new notification requirements on businesses exposed to a data breach. The amended law requires businesses to notify affected individuals within 45 days after the breach whenever the breach is reasonably likely to subject consumers to a risk of harm. It also specifies the information that must be included in customer notifications, including basic information to help consumers secure or recover their identities, such as the contact information for consumer reporting agencies. The amended law also expands coverage to include hard copy data (in addition to computerized data) and removes a blanket exemption for encrypted data, clarifying that a breach of encrypted data can trigger notification requirements if the encryption key or other decryption tools are acquired during the breach. The full text of Washington's law as amended, which becomes effective in July 2015, is available here.

North Dakota amended its security breach notification law to require any person or business that experiences a breach of its security system affecting more than 250 individuals to disclose the breach to the state Attorney General. The amendment narrows the definition of "personal information" as it pertains to employee data. Now, a breach that compromises an individual's employee identification number will only give rise to notification obligations if the breach also affected "any required security code, access code, or password" accompanying the number. The full text of North Dakota's amended law is available here.

Virginia announced the creation of the first state-level Information Sharing and Analysis Organization (ISAO), a new governmental organization intended to facilitate the collection and sharing of information related to cybersecurity threats and attacks. In addition, Virginia's governor signed the "Securing Consumer Transactions" directive on May 5, which encourages statewide adoption of advanced electronic payment security technologies, including "chip-and-pin" authentication features. It directs the state's technology and finance secretaries, treasurer, and comptroller to (1) update the state's main purchase card program to include chip-and-pin technology by the end of the year, and (2) develop a plan to enhance the security features of merchant and prepaid debit card programs by October 1, 2015. The full text of the governor's directive on payment security is available here. The governor's press release announcing Virginia's ISAO is available here.