Bond

INFORMATION MEMO
CYBERSECURITY AND DATA PRIVACY

NOVEMBER 2016

Federal Agencies Issue New Guidelines and Rules for Data Breaches and Online Security

After recent high profile data breaches and threats to online privacy—ranging from Yahoo Inc.'s data breach of approximately 500 million accounts to the hacking of Hillary Clinton's campaign manager, John Podesta's email accounts—three federal agencies are being more proactive in advising businesses and consumers of better ways to protect themselves.

The Federal Trade Commission (FTC) recently issued a guide for businesses on handling data breaches. The 16-page guide outlines some of the processes and procedures a company must consider when a data breach is confirmed or suspected. For instance, the FTC recommends that a business must first secure its operations by assembling a team of experts and consulting with legal counsel to ensure that the initial breach is contained. The next step is to fix any vulnerability within the system's network by working with forensic experts, to verify the types of information compromised and recommend necessary remedial measures. The guide also encourages businesses to formulate a comprehensive communications plan, wherein all affected parties—employees, customers, and business partners—can obtain information to protect themselves. The final step is to notify the appropriate parties: businesses must determine their legal requirements for the types of information involved in the breach, notify law enforcement, and notify affected third parties. To assist businesses through the notification process, the FTC also supplies a model notification letter for reference. Although not exhaustive, the list provides some organization to the process of addressing a data breach issue.

On October 27, 2016, the Federal Communications Commission (FCC) issued new rules in favor of online privacy, limiting how Internet Service Providers (ISPs) use and sell consumer data, and providing customers with more control over their personal information. ISPs have access to valuable personal data from their users, such as browsing history and precise geolocation data, which can be packaged and sold to data brokers and marketers without the consumer's knowledge or permission. Under the FCC's new rules, however, ISPs must inform consumers as to what information is collected and how it is being used or shared, and ISPs must also obtain the consumers' permission—referred to as "opt-in consent"—to share the information. Although these new rules are being met with some resistance, ISPs will have a year to comply with the new regulations.

Finally, the U.S. Department of Health and Human Services (HHS) recently issued new guidance on handling ransomware. Ransomware is a form of attack where the hacker encrypts a company's files so they cannot be accessed. The hacker then demands that the victim pay a ransom for the encryption key. If the victim fails to pay this ransom by a certain deadline, they may forever lose access to their information. The HHS, in an attempt to limit the damage from ransomware attacks, issued guidance to strengthen the cybersecurity standards of entities covered under the federal Health Insurance Portability and Accountability Act (HIPAA). The guidance provides that those subject to HIPAA must "implement policies and procedures that can assist an entity in responding to and recovering from a ransomware attack." For example, entities are encouraged to maintain frequent backups and conduct periodic test restorations, in order to ensure that an entity's data cannot be held hostage to a ransomware attack. Although the HHS guidelines were drafted for healthcare entities, the guidelines are also instructive for enterprises in all sectors.

If you have any questions about this Information Memo, please contact Clifford G. Tsan, Michael D. Billok and Franz M. Wright or the attorney in the firm with whom you are regularly in contact.

BOND SCHOENECK & KING ATTORNEYS

Commitment · Service · Value · Our Bond