Encryption is Key to Limiting Company Exposure for Data Security Breaches

Karen H Bromberg, Partner

Duane A Cranston, Associate

Companies doing business in California may find themselves targeted for investigation if they fail to encrypt personal information, according to a recent report issued by the California Attorney General's office. Last week, California Attorney General Kamala D. Harris released a report stating that the AG's Office will investigate breaches involving unencrypted personal information and urged law enforcement agencies to prioritize these investigations, noting that data breaches in California exposed more than 2.5 million residents to the risk of identity theft in 2012 and that 1.4 million Californians could have been protected from this risk had their personal data been encrypted. "Data breaches are a serious threat to individuals' privacy, finances and even personal security," Harris said. "Companies and government agencies must do more to protect people by protecting data."

The report's recommendations are intended to strengthen and supplement the protections established by California's 2002 data breach notification law (Cal. Civ. Code 1798.82 and 1798.29) (the "Breach Notification Law"). These laws require government agencies and private companies, respectively, to disclose any breach of unencrypted security information to any California resident whose personal information has been, or is reasonably believed to have been, acquired by an unauthorized person. Although the Breach Notification Law provides a safe harbor for companies which encrypt personal data by exempting them from the statute's notification requirements, according to the AG, this "carrot" has not been a sufficient motivator: organizations are still not encrypting personal information and consequently are "subjecting too many Californians to a risk that is eminently avoidable."

The AG also recommended enacting a law to require the use of encryption to protect personal information on portable devices, media and in email and suggested that "an appropriate encryption standard might be FIPS 197, the National Institute of Standards and Technology's standard approved for U.S. Government organizations to protect higher risk information."

Encryption was not the report's entire focus. The AG also recommended additional security and disclosure measures for companies storing or transmitting personal information from their secure networks. These measures include requiring companies to:

- Review and tighten security controls on personal information, including security training for the company's employees and contractors;
- Make breach notices more plainly comprehensible to individuals whose data may have been compromised;

- Offer damage mitigation products, such as credit card monitoring, and provide information on other protective measures to individuals whose social security and/or driver's license numbers have been exposed; and

- Notify individuals when there has been a breach of online security credentials (e.g. user names and passwords).

The AG's recommendations also include broadening disclosure requirements under the Breach Notification Law to require the disclosure of any breach of online credentials such as usernames and passwords. Such information is not presently deemed "personal information," as defined in the statutes. The report notes that such breaches not only create vulnerabilities for personal and corporate security, but can also be exploited to launch cyber-attacks on public infrastructure and government networks.

The recommendations in the report, if enacted, would set a substantially higher standard for the storage and transmission of personal information. Companies should consider getting ahead of this trend by upgrading their network and security measures and policies, including developing data encryption for transmitting personal data and providing employee training on data security policies and procedures.

About the Authors

Ms. Bromberg is the head of the firm's Intellectual Property and Technology group. She handles all aspects of intellectual property, Internet, privacy, data security and technology law, including license agreements, technology transfer and vendor agreements, joint development and co-branding agreements, website terms of service, and management of IP litigation (including patent, trademark, copyright, and trade secret litigation). She was named as a New York *Super Lawyer* for Intellectual Property in 2010, 2011, and 2012.

Mr. Cranston is an associate in the firm's Intellectual Property and Technology, Corporate, and Litigation and Arbitration groups. Mr. Cranston's practice includes serving as outside general counsel for general corporate and intellectual property matters as well as counseling on privacy and data security issues. He graduated *cum laude* from Harvard University and earned his J.D. from Columbia Law School. Prior to joining the firm, Mr. Cranston was a Senior Director of Business Affairs at ESPN and practiced at Cravath, Swaine & Moore.

About Cohen & Gresser

Founded in 2002, Cohen & Gresser LLP has been recognized in *Chambers USA*, *Legal 500*, and *Benchmark Litigation* and was recently named to *The National Law Journal*'s 2013 "Midsize Hot List." The firm has offices in New York and Seoul and has grown to over fifty lawyers in four practice groups: Litigation and Arbitration; Corporate Law; Intellectual Property and Technology; and White Collar Defense, Regulatory Enforcement and Internal Investigations. Its attorneys are graduates of the nation's best law schools and have exceptional credentials, and its clients include Fortune 500 companies and major financial institutions throughout the world.

NEW YORK | SEOUL

www.cohengresser.com info@cohengresser.com PH: +1 212 957 7600

July 9, 2013