BAR BULLETIN

KCBA KING COUNTY BAR ASSOCIATION

Justice... Professionalism... Service... Since 1886

This is a reprint from the King County Bar Association Bar Bulletin

January 2016

Safeguarding Personal Information:

What Washington Businesses Need To Know about Data Security Standards

By Charles E. Harris II, Laura R. Hammargren and Rebecca M. Klein

It was recently reported that, prior to the end of the year, there had been 717 data breaches in 2015, exposing an estimated 176 million records. Thirteen of the breaches targeted Washington-based organizations.[1]

The hefty financial costs and reputational harm that usually attend these attacks have raised awareness about the importance of data security at the highest levels in organizations. But, with no national law establishing mandatory, uniform data security measures, many organizations are unsure about whether they are legally required to employ specific safeguard standards.

This article discusses safeguard standards under: (i) federal law; (ii) the Revised Code of Washington (RCW); and (iii) laws from other states. The article also discusses certain established data security standards and why Washington entities — even those subject to statutory safeguard standards — might consider complying with one of these standards.

U.S. businesses in only a few sectors have traditionally been subject to specific data security standards under federal law. The two primary examples are "financial institutions" and companies that handle health care information. If a business is not part of or dealing frequently with these sectors, there are generally no specific safeguard standards that a business must implement pursuant to federal statute.

Some state statutes, however, require specific safeguards for companies that do business in the state or that handle personal information of the state's residents. Moreover, companies may be contractually required to implement specific data security standards. For example, credit card brands, including Visa, MasterCard, American Express and Discover, require businesses that store and transmit payment card data to comply with the Payment Card Industry Data Security Standard (PCI-DSS).

Industry-Specific Federal Data Security Standards

Financial Institutions

The Gramm-Leach-Bliley Act (GLBA)[2] declared it a public policy that each "financial institution" has an affirmative obligation to "protect the security and confidentiality of [its] customers' nonpublic personal information."[3] A "financial institution" under the GLBA includes any entity "engaging in financial activities."[4]

The GLBA does not contain specific data security standards. Instead, it tasks certain federal and state agencies with establishing appropriate standards for financial institutions subject to their jurisdiction.[5]

The FTC, for example, promulgated the "Safeguards Rule" under the GLBA.[6] The Safeguards Rule, which applies to any business covered by the GLBA that is "significantly engaged" in providing financial products or services,[7] mandates that these businesses develop a written information security program (or WISP) containing the following elements:

- Identification and assessment of the risks to customer information in relevant company operations, and evaluation of the effectiveness of the current safeguards;
- Implementation of safeguards to control the risk identified in the assessment;
- Regular testing and monitoring of the WISP's effectiveness;
- Oversight of the handling of customer information by service providers and the selection of service providers that can maintain appropriate safeguards;
- Evaluation and adjustment of the program in light of relevant circumstances, including changes in operations or the results of security testing and monitoring; and
- Establishment of procedures to properly dispose of personal information.[8, 9]

Businesses in the Health Care or Medical Industry

Similarly, the Health Insurance Portability and Accountability Act (HIPAA) requires businesses in the health care industry that store or transmit health information to maintain reasonable and appropriate safeguards to protect personal information.[10] Entities covered under HIPAA include health care plans and clearinghouses, and health care providers that transmit health information in electronic form.[11]

As mandated by HIPAA, the Department of Health and Human Services (HHS) promulgated its "Security Rule."[12] This Security Rule establishes a national set of security standards for protecting health information that is held or transferred in electronic form ("ePHI"). It requires that health care companies incorporate certain elements into their HIPAA security compliance plan, including the following:

• Administrative safeguards, such as (i) implementing procedures that outline sanctions for data security violations, and (ii) developing procedures regarding access to ePHI;

• Physical safeguards, such as (i) limiting physical access to equipment that contains ePHI, and (ii) describing how workstations with access to ePHI are secured;

• Technical safeguards, such as (i) controls for limiting access to ePHI, e.g., encryption, and (ii) mechanisms to protect ePHI transmitted electronically.[13]

Washington Law

RCW § 19.255.020, enacted in 2010, gives payment card-issuing banks a claim against certain entities that are negligent in safeguarding payment card data.[14] The law applies to:

(i) businesses that provide goods or services to Washington residents and process more than 6 million payment card transactions annually;

(ii) payment processors that process or transmit payment card account information; and

(iii) vendors that maintain this account information on behalf of third parties.[15]

In the event of a data breach, a business or payment processor is "liable to [an issuing bank] for reimbursement of reasonable actual costs related to the reissuance of credit cards and debit cards" to Washington customers *if* the business or payment processor "fails to take reasonable care to guard against unauthorized access to account information that is in the possession or under the control of the business or processor, and the failure is found to be the proximate cause of a breach."[16]

Also, a vendor is liable to the financial institution if its "damages were proximately caused by the vendor's negligence."[17] However, section 19.255.020 provides a "safe harbor." The entities described above are not liable to a financial institution for damages caused by a breach if: (i) "the account information was encrypted at the time of the breach" or (ii) the entity "was certified compliant" with the most recent version of PCI-DSS.

Data Security Standards under Other State Laws

The following three states have enacted laws establishing specific data security standards that may apply to Washington entities engaging in interstate transactions with those state's residents.

Massachusetts

The Massachusetts Standards for the Protection of Personal Information apply to any entity that "receives, stores, maintains, processes, or otherwise has access to personal information" of that state's residents in connection with "the provision of goods or services" or "employment."[18] Such entities must implement a comprehensive WISP containing: (i) many of the standards discussed above; and (ii) certain technical safeguards contained in safeguard rules of federal agencies.[19]

Nevada

Nevada's Security of Personal Information statute applies to any entity that "handles, collects, disseminates or otherwise deals with nonpublic personal information" of Nevada residents.[20] The Nevada statute provides that an entity possessing records containing the personal information of its residents must: (i) implement reasonable security measures; (ii) include a provision in service provider contracts requiring that they implement proper measures; and (iii) take reasonable measures to destroy those records.[21]

Moreover, businesses doing business in Nevada that do not accept payment cards must encrypt records containing personal information,[22] whereas those businesses that do accept payment cards for goods and services *must* comply with the current version of PCI-DSS.[23] The Nevada statute also creates a "safe harbor" for businesses in compliance with the encryption requirements or PCI-DSS.[24]

Minnesota

The Minnesota Plastic Card Security Act (PCSA) applies to any entity that: (i) conducts business in Minnesota; and (ii) accepts payment cards in connection with transactions. It mandates that covered entities must not retain the following customer data after "authorization of the transaction:" (i) the card security code data; (ii) the personal identification code (PIN) number verification code number; and (iii) the full contents of any track of magnetic strip data from the payment card.

As for "PIN debit transactions, the described data must not be retained following 48 hours after authorization of the transaction." The PSCA provides that a business is strictly liable for the costs incurred by financial institutions resulting from a breach if the business's or its service provider's system is breached, and either has violated the PSCA.

Established Data Security Standards

There are many frameworks, standards and best practices that a business may choose to employ to protect personal information. Aside from PCI-DSS, two of the more well-known standards are those published by the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).

In February 2014, NIST released the first version of its "Framework for Improving Critical Infrastructure Cybersecurity." This framework provides a structure that businesses and regulators can use to create, assess or improve data security programs.

The latest ISO standard, "ISO/IEC 27002," which was developed and published in October 2013, offers best practice recommendations on data security management to be used by professionals who are responsible for maintaining information security management systems.

While compliance with a particular data security standard may not be required by law or contract, businesses may want to employ one of these standards for several reasons:

• To make a company's systems more secure from cyber attacks and help mitigate losses if a breach occurs;

• To increase the company's con-

sumer confidence and improve the company's reputation with its business partners;

• To comply with applicable laws and regulations.

• To help a company establish that it implemented "reasonable" security measures to protect personal information if the company is faced with litigation following a cyber attack; and

• To assist in avoiding scrutiny from federal agencies or state attorneys general. The government has brought enforcement actions based on businesses failing to implement more robust data security measures.[25] ■

Charles E. Harris, II, a partner in Mayer Brown's Litigation & Dispute Resolution Practice Group, defends companies in data-breach class actions and counsels clients regarding compliance with data-safeguarding guidelines and creating information security programs.

Laura Hammargren is an associate in Mayer Brown's Litigation & Dispute Resolution Practice Group in the firm's Chicago office. In her investigations practice, she represents corporations and individuals in internal investigations or who are under investigation by federal and state authorities for securities fraud, health care fraud, Foreign Corrupt Practices Act (FCPA), and False Claims Act (FCA) violations.

Rebecca Klein is a litigation & dispute resolution associate in Mayer Brown's Chicago office. Prior to joining Mayer Brown, Klein clerked for the Hon. Milton I. Shadur of the U.S. District Court for the Northern District of Illinois.

[1] Identity Theft Resource Center, "Data Breach Reports" (Dec. 1, 2015), available at: *http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf.*

[2] 15 U.S.C. § 6801 *et seq.*

[3] *Id.* § 6801(a).

[4] *Id.* § 6809(3) (incorporating 12 U.S.C. § 1843(k)).

[5] *Id.* § 6801(b).

[6] 16 C.F.R. Part 314.

[7] *Id.* § 314.2(a) (incorporating 16 C.F.R. § 313.3(k)).

[8] *Id.* § 314.4.

[9] For a comprehensive discussion about data security standards promulgated by other federal and state agencies pursuant to the GLBA, please see Mayer Brown's white paper "Big Data and Cybersecurity: Standards for Safeguarding Personal Information," available at: *https://m.mayerbrown.com/big-data-and-cybersecurity-standards-for-safeguarding-personal-information-10-20-2015/.*

[10] 42 U.S.C. § 1320d-2(d)(2).

[11] *Id.* § 1320d-1(a).

[12] 45 C.F.R. Part 164, Subpart C.

[13] *Id.* §§ 164.308, .310, .312, .314, .316.

[14] RCW § 19.255.020(3)(a), (b).

[15] RCW § 19.255.020(2), (3).

[16] RCW § 19.255.020(3)(a).

[17] RCW § 19.255.020(3)(b).

[18] 201 C.M.R. 17.02.

[19] *Id.* § 17.03.

[20] Nev. Rev. Stat. § 603A.030.

[21] *Id.* §§ 603A.210(1), (2), .200(1).

[22] *Id.* § 603A.215(2).

[23] *Id.* § 603A.215(1).

[24] *Id.* § 603A.215(3). No court has considered the scope of this immunity under the Nevada statute, but a party seeking to limit its reach would probably contend that the immunity applies where Nevada provides the applicable law, or personal information of Nevada residents is compromised.

[25] *E.g., In the Matter of Superior Mortgage Corp.*, F.T.C. No. 02 3136 (filed Dec. 16, 2005).