

STANDING IN THE BREACH— STATE LAW REQUIREMENTS WHEN A CUSTOMER DATA BREACH OCCURS

By: *Shane B. Hansen and Jordan Paterra*
Warner Norcross & Judd LLP

Safeguarding the customer information in your firm's possession is not just a good business practice, it is required under federal law and related rules.¹ One year ago, the Securities and Exchange Commission ("SEC") published for comment proposed amendments to Regulation S-P, *Privacy of Consumer Financial Information and Safeguarding Personal Information*,² that would expand upon those requirements and impose specific obligations upon firms when a breach of their data security occurs.³ The SEC's adoption of these requirements is not an "if," but a "when." The federal banking regulators jointly adopted the Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice that is applicable to banks in March 2005.⁴ Safeguarding customer information and preventing identity theft are among the SEC's and FINRA's regulatory priorities for 2009.⁵ Firms are presently grappling with their implementation of the "Red Flag" rules, effective May 1, 2009, promulgated by the Federal Trade Commission⁶ which are generally applicable across industry boundaries.⁷ But your challenges do not end with federal privacy laws and related rules.

Forty-four states have filled a perceived gap in consumer protection by requiring notification of security breaches under various circumstances.⁸ Twenty-nine of these state laws contain exceptions or safe harbors for firms that are subject to, and/or comply with, federal privacy laws and related rules promulgated by their primary federal regulator.⁹ The contours of these exceptions and safe harbors vary among the states and some appear to depend upon the

¹ Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq.; see also Financial Privacy Act, 12 U.S.C. § 3401, et seq.; Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.; the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191; and 2 Richard L. Fischer, *The Law of Financial Privacy* § 5.01 (2007).

² Part 248 – Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information, Release Nos. 34-57427; IC-28178; IA-2712; File No. S7-06-08 (3-4-08).

³ For a discussion of the SEC's proposed amendments, see *NSCP Currents*, April/May 2008, *The Price of Protecting Privacy—Proposed Regulation S-P Amendments*, by Shane B. Hansen.

⁴ See www.occ.treas.gov/consumer/Customernoticeguidance.pdf.

⁵ See FINRA's 2009 exam priorities letter at <http://www.finra.org/web/groups/industry/@ip/@reg/@guide/documents/industry/p118113.pdf> and the SEC's CCO Outreach National Meeting Agenda at <http://www.sec.gov/info/bdccooutreach.htm>.

⁶ The FTC and the federal banking regulators issued joint regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act) www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf.

⁷ For broker-dealers, see FINRA Regulatory Notice 08-69 *Fair and Accurate Credit Transactions Act of 2003*. Besides banking institutions, the term "financial institution" includes "any other person that, directly or indirectly, holds a transaction account . . . belonging to a consumer." 16 CFR 681.2(b)(7); 15 U.S.C. § 1681a(t).

⁸ See National Conference of State Legislatures website for a list and links with the states at: <http://www.ncsl.org/programs/lis/cjp/priv/breachlaws.htm>. States with no security breach law include Alabama, Kentucky, Mississippi, Missouri, New Mexico, and South Dakota.

⁹ The following 15 states' breach notification laws do not contain an exception or safe harbor for compliance with federal law or related rules governing data breaches: California, District of Columbia, Georgia, Illinois, Louisiana, Montana, New Jersey, New York, North Carolina, North Dakota, Ohio, Oklahoma, Texas, Vermont, and Washington. See also New York City ordinances.

SEC's final adoption of rules requiring security breach notifications. Fifteen states' laws do not contain exceptions or safe harbors based on compliance with an SEC rule. Forty-seven states have enacted "security freeze" laws allowing customers to freeze their credit reports in the event of a security breach.¹⁰

State security breach statutes impose similar, yet somewhat inconsistent, obligations on firms for reporting data breaches.¹¹ If a firm services customers in multiple states, then it will be forced to follow differing state laws and reporting obligations to different customers—a daunting task when a firm may service customers in many or all fifty states. Many, many questions arise once you start digging into these state breach notification laws. Federal privacy laws and related rules do not preempt these state laws.

Does your firm have to report data breaches?

The first question should be an easy one, yet, even with this threshold question, different states require different persons to report data breaches. California was among the first to address these issues.¹² A majority of states follow California's reporting approach, which requires any firm that conducts business in California to report a data breach if that firm owns, licenses, or maintains data that is covered by the law ("covered data"). Some states have added their own spin to California's approach. They require any person, whether or not conducting business within the state, to report a data breach if that person owns, licenses, or acquires covered data regardless of where the individual described in the data resides if the state has any basis to assert its jurisdiction.¹³ Other states are more clearly focused on protecting their own citizens and require a data breach to be reported if the person owns or licenses computerized data that includes personal information of an individual residing in the state.¹⁴

Several states also require that "data collectors" or any person that, for any purpose, handles, disseminates, or otherwise deals with nonpublic personal information report data breaches.¹⁵ Some states require any person that deals with personal information to report a data breach.¹⁶ Hence, more than one state's law may apply and more than one person with responsibility for the data (a "covered person") may have a reporting obligation for the same data breach.

¹⁰ http://www.consumersunion.org/campaigns/learn_more/003484indiv.html (last visited March 10, 2009).

¹¹ See, for example, *Navigating Some Uncertain Waters in Michigan's New Security Breach Notification Law*, Norbert F. Kugele and James Placer (July 2007) at: http://www.wnj.com/nfk_privacy_and_data_security_law_journal_article_july_2007/

¹² Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.). California was the first state to create an agency devoted to consumer privacy issues, the California Office of Information Security and Privacy Protection, on the Internet at http://www.oispp.ca.gov/consumer_privacy/default.asp.

¹³ See, e.g., Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.).

¹⁴ See, e.g., Md. Code Ann., Com. Law § 14-3501 to -3508 (2007 Supp.).

¹⁵ See, e.g., 815 Ill. Comp. Stat. 530/1 to /30 (2007 Supp.); Vt. Stat. Ann. tit. 9, § 2430 to -2435 (2006).

¹⁶ See, e.g., Mass. Gen. Laws 93H § 1-6 (2007); 2007 Or. Laws 759.

What is “personal information”?

State breach notification statutes defining “personal information” have an assortment of terms affecting the scope of breach notification requirements. The California statute is the model for most states. The California statute defines “personal information” as a combination of a first name, or first initial and last name, in combination with any one or more of the following data elements, when either the name or data elements are not encrypted: social security number; driver’s license number or state identification number; or account number, credit or debit card number in combination with any required security code, access code, or password permitting access to an individual’s financial account. California has amended this definition to also include medical and insurance information. California does not consider “personal information” to include any information available to the general public from federal, state, or local government records.¹⁷ Other states expand their definition to include the following as “personal information”: medical information; middle name; or information sufficient to perform identity theft.¹⁸ Some states follow California and do not consider publicly available information as “personal information,” while other states do not have such an exception in their definitions.¹⁹

Does your firm have an affirmative obligation to protect data?

Depending on the state in which your firm does business, or where your customers reside, your firm may have an affirmative obligation to protect data.²⁰ States vary in this affirmative obligation. California does not impose an obligation to protect data while other states require reasonable measures to protect against unauthorized access, while still other states require reasonable security measures and an affirmative obligation to destroy customer records after use.²¹ Some states do exempt financial institutions (not always defined the same way) from an obligation to use reasonable measures to destroy customer records after use,²² but federal law and related rules impose similar obligations.²³

What constitutes a breach?

The way a state statute defines “breach” of data and what the statute requires of a firm once a breach has occurred often leads to inconsistent reporting obligations for a firm. A data breach in one state may not be a data breach in another state. As a result, a firm would have to

¹⁷ Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.).

¹⁸ See, e.g., Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.); Fla. Stat. ch. 817.5681 (2006); Ga. Code Ann. §§ 10-1-910 to -912 (2007 Supp.).

¹⁹ See, e.g., Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.).

²⁰ See, e.g., Code of Massachusetts Regulations at 201 CMR 17.00, “Standards for the Protection of Personal Information of Residents of the Commonwealth,” effective in three stages starting on 1/1/2009, issued under Massachusetts General Laws chapter 93H, which addresses information security breaches.

²¹ See, e.g., Haw. Rev. Stat. §§ 487N-1 to -4 (2007 Supp.); Md. Code Ann.; Com. Law § 14-3501 to -3508 (2007 Supp.) (requiring reasonable measures to protect against unauthorized access); Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.); Mont. Code Ann. § 30-14-1704 (2007); Nev. Rev. Stat. § 603A.220 (2007 Supp.) (requiring reasonable security measures and an affirmative obligation to destroy customer records after use).

²² See, e.g., Tex. Bus & Com. Code Ann. § 48.103 (2007 Supp.); Utah Code Ann. § 13-44-101 (2007 Supp.).

²³ Financial Privacy Act, 12 U.S.C. § 3401, et seq.; Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.; Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq.

report what one state defines as a data breach to customers only of that state, when, in actuality, the data breach could have impacted more customers in different states. Firms may choose to report data breaches to some customers in some states, even when not required, for simplicity and consistent treatment of all customers.

Again California serves as the model for many states. California defines a “breach” as the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a firm.²⁴ This approach focuses on the recipient, rather than the loss of data by the firm or its agents. As a variation of the California model, some states define a breach as access and acquisition of covered data that is reasonably likely to cause substantial economic loss to an individual or is not likely to cause reasonable harm after an investigation.²⁵ Other states require that the breach be a “material” compromise of the data in combination with an unlawful acquisition by the recipient.²⁶

Does it matter that your data is in paper or electronic formats?

A majority of states require covered persons to report breaches involving unencrypted computerized personal information or a variation of this type of data.²⁷ Other states apply a broader approach to covered data, requiring persons to report data breaches not only of computerized personal information, but computerized data transferred to a different medium, such as paper; and other states also require data breach notification even of written, drawn, spoken, visual, or electromagnetic information.²⁸ States also differ with respect to whether breach notification is required when the data is in an unencrypted form or when encrypted with an encryption key. Some states require persons to report all forms of breached data.²⁹

What notification is required?

After a breach has occurred, California requires a firm to notify a California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.³⁰ Other states do not have such a state specific notification law requirement. Where a breach has occurred, some states require firms to notify “affected individuals,” with no limit as to whether the individuals reside in a specific state.³¹ Some state statutes do not require notification if there is no reasonable likelihood of harm to customers after an investigation, while other states require firms to notify customers upon discovery or knowledge of a breach regardless of its potential impact on them.³²

²⁴ Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.).

²⁵ See, e.g., Ariz. Rev. Stat. § 44-7501 (2007 Supp.); Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.).

²⁶ See, e.g., Fla. Stat. ch. 817.5681 (2006).

²⁷ Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.).

²⁸ See, e.g., Haw. Rev. Stat. §§ 487N-1 to -4 (2007 Supp.); Ind. Code §§ 24-4.9-1-1 to -3-4 (2006).

²⁹ See, e.g., Mass. Gen. Laws 93H § 1-6 (2007)

³⁰ See, e.g., Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.); Mich. Comp. Laws § 445.71 (2007 Supp.).

³¹ See, e.g., Ariz. Rev. Stat. § 44-7501 (2007 Supp.).

³² See, e.g., Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.); Col. Rev. Stat. § 6-1-716 (2007 Supp.); Fla. Stat. ch. 817.5681 (2006); (not requiring notification if there is no reasonable likelihood of harm to customers after an investigation); 815 Ill. Comp.

How quickly does your firm have to report?

State statutes also determine the timeliness in which your firm must notify your customers. Although California requires you to notify your customers in the most expedient time possible and without unreasonable delay, generally within 10 days, California also allows your firm to delay if a law enforcement agency determines that the notification would impede a criminal investigation.³³ Other states do not require the “most expedient time possible” while others allow for a delay of notification to restore the integrity of the data breached computer system to prevent the risk of further unauthorized access before making the announcement.³⁴ Wisconsin requires a “reasonable time” not to exceed forty-five days after learning of the breach. Wisconsin takes into consideration the number of notices and the method in which a firm can notify customers.³⁵ North Carolina requires notification without unreasonable delay, consistent with legitimate needs of law enforcement and consistent with any measures necessary to determine sufficient contact information, scope of breach and restore the reasonable integrity, security, and confidentiality of the data system.³⁶ On the other hand, Maryland also requires that notification be sent to its Office of Attorney General prior to communicating with affected consumers, which posts these notifications on its website.³⁷

Who can sue your firm for failure to comply with data breach statutes?

State statutes take three different approaches with regards to who can enforce the state data breach statutes. The first approach is that injured customers themselves can bring civil actions against your firm.³⁸ The second approach is that the state statute specifies certain government entities to enforce the statutes, such as the state attorney general or designated state departments.³⁹ The final approach is a blend of the first two, where both private and state enforcement may bring actions against persons that fail to comply with the state data breach statutes.⁴⁰

Some states offer a safe harbor for compliance with other states’ statutes.

Despite conflicting, overlapping, or contradictory state data breach statutes, some states offer safe harbors recognizing that other states’ laws may also apply and some recognize that

Stat. 530/1 to /30 (2007 Supp.) (require businesses to notify customers upon discovery or knowledge of a breach regardless of its potential impact on them).

³³ Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.).

³⁴ See, e.g., Col. Rev. Stat. § 6-1-716 (2007 Supp.).

³⁵ See, e.g., Wis. Stat. § 895.507 (2006).

³⁶ See, e.g., N.C. Gen. Stat. § 75-65 (2007).

³⁷ Maryland Personal Information Protection Act, MD Stat. Ann. § 14-3504. See <http://www.oag.state.md.us/idtheft/businessGL.htm>.

³⁸ See, e.g., Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.); Minn. Stat. § 325E.61 (2007 Supp.); Tenn. Code Ann. § 47-18-2107 (2007 Supp.).

³⁹ See, e.g., Ariz. Rev. Stat. § 44-7501 (2007 Supp.); Me. Rev. Stat. Ann. tit. 10, §§ 1346 to 1350-A (2007 Supp.); 2007 Or. Laws 759.

⁴⁰ See, e.g., Haw. Rev. Stat. §§ 487N-1 to -4 (2007 Supp.); N.H. Rev. Stat. Ann. §§ 359-C:19 to :21 (2007 Supp.).

firms may implement a more protective approach to data breaches. The California statute deems that a firm has complied with the data breach statute if a firm maintains their own notification procedures as part of an information security policy that is consistent with California's timing requirements.⁴¹ Colorado's statute excepts firms that already comply with federal or state laws that require security breach notification procedures.⁴² Delaware has the same exception and also excepts broadly those persons that maintain their own notification procedures.⁴³

Once a breach has occurred, can customers freeze their credit report file?

Once a data breach has occurred, 47 states and the District of Columbia have enacted security freeze laws which allow customers to freeze their credit report file. Security freeze laws prohibit a credit reporting agency from releasing information from a file without "the express authorization of the consumer."⁴⁴ State security freeze laws also vary widely as to who may enact the security freeze, if there is an exception for insurance, how much the security freeze costs, whether a customer can lift a security freeze for a specific party, and whether there is a charge to lift the freeze for a specific period or a specific party. States have two approaches as to whom the security freeze laws cover. The first approach taken by a minority of states is to allow only identification theft victims to use the freeze laws.⁴⁵ The second approach allows any consumer to use the security freeze laws when there has been a data security breach.⁴⁶ States take a varied approach as to charges for freezes and lifting of the freeze for a period of time or indefinitely. States also take a varied approach as to whether it will allow a customer to lift a freeze for a specific amount of time or for a specific party.

What should your firm do?

For most firms, it is probably not an "if" but a "when" the security breach occurs. Planning for the event will improve your response time, which may help you mitigate the potential damages resulting from a data breach. The first step is to understand your federal and home state's security data breach notification and freeze laws, as well as the state laws where your customers reside. Your firm must understand these laws in order to know what type of data is covered under the statute, when a reportable breach has occurred, and what type of reporting regimen the state requires of your firm.

You need to assess the data security risks facing your firm and analyze where and how a breach could occur. Consider everything from high tech to low tech possibilities. This process will be most effective if you organize a working group of knowledgeable employees in your firm who understand your technology and data storage systems and processes, as well as paper copies of your books and records.

⁴¹ Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.).

⁴² See, e.g., Col. Rev. Stat. § 6-1-716 (2007 Supp.); Me. Rev. Stat. Ann. tit. 10, §§ 1346 to 1350-A (2007 Supp.).

⁴³ See, e.g., Del. Code Ann. tit. 6, §§ 12B-101 to -104 (2005).

⁴⁴ 2 Richard L. Fischer, *The Law of Financial Privacy* § 5.07 (2007).

⁴⁵ See, e.g., Ark. Code Ann. §§ 4-110-101 to -108 (2007 Supp.); Kansas Stat. §§ 50-7a01 to -7a04 (2007 Supp.).

⁴⁶ See, e.g., Cal. Civ. Code §§ 1798.80-1798.84 (2007 Supp.); Conn. Gen Stat. § 36a-701b (2007 Supp.); Del. Code Ann. tit. 6, §§ 12B-101 to -104 (2005).

After identifying the risks, develop a plan to address and manage those risks. Periodically review and update your risk assessment, particularly when you make significant changes to your computer systems and business processes that involve customer data. These records will be requested by the SEC and/or FINRA during the examination process. Also, remember that these are ordinary business records that are discoverable in litigation, so you should consider involving your legal counsel in this self-assessment process.

Depending on the size and complexity of your firm, consider organizing a standing “SWAT Team” of employees in your organization who understand your technology and data storage systems and processes. Your SWAT Team should meet and develop several hypothetical data breach mock drills with scenarios to help you think through and develop written procedures to respond when the real thing occurs.

These planning exercises, together with the related documentation, will help you create a comprehensive data security breach notification system. With a system in place, your firm may be able to take advantage of the safe harbors created by many, but not all, of the state laws that regulate these circumstances. Most importantly, by taking these steps your firm may be able to better protect your customers and your reputation and, hopefully, avoid regulatory enforcement proceedings.