

Practitioner's Perspective

by Holly K. Towle, J.D.



Holly K. Towle is a partner with Kirpatrick & Lockhart Preston Gates Ellis LLP (K&L Gates), an international law firm, and chair of the firm's E-merging Commerce group. Holly is located in the firm's Seattle office and is the coauthor of *The Law of Electronic Commercial Transactions* (2003, A.S. Pratt & Sons). Holly.Towle@KLGates.com, 206-623-7580.

Practitioner's Perspective appears periodically in the monthly Report Letter of the CCH Guide to Computer Law. Various practitioners provide in-depth analyses of significant issues and trends.

What Will You Do When You Get the Dreaded Call, "We've Had a Data Security Breach!"

You just received a call that you've had a data security breach and personal information on your customers, employees or others may have been accessed without authorization or might otherwise be exposed. Your IT services department is now taking steps to prevent further attack.

What do you do next? This article provides a "cheat sheet" to help you through the initial response steps and to gather information needed to determine what law applies and whether it requires you to provide notice of the breach.

Initial Steps

The first thing to do is to stop the IT folks from making any missteps. Unless they have sufficient forensic expertise, you may need or want to engage an outside data security firm to help: steps taken to prevent further breach should not destroy evidence or erase the trail needed to determine what happened. Better yet, have your attorneys engage the data security firm so that the investigation may be part of the confidentiality privilege pertaining to the information moving back and forth with your attorneys. None of this should delay containing and controlling the incident ASAP – the point is that there are good ways and bad ways to do that.

And yes, you will need an attorney. Over 35 states have data security breach notice laws and they're all different. The federal government also has rules from various regulators and they're different as well. For example, the above suggestion not to destroy evidence is not really just a suggestion—if your company is covered by guidance from certain federal regulators, preserving evidence is one of the components of the security breach response plan that you're supposed to have in place right now.¹

Call a law firm that deals with privacy and data security laws generally (not just data security triage) and that has a broad enough practice to help with subsequent issues. Working through a data security incident typically reveals latent legal issues (*e.g.*, employment policies, web site terms of use and privacy and security policies, customer agreements, and service contracts all might need to be revised) or creates new issues that will need to be addressed after the incident is long gone. If the breach is significant enough, you may ultimately need securities law attorneys (*e.g.*, to advise re securities filings for public companies), litigators (to handle the lawsuits that can follow the security incident), and commercial law attorneys who are familiar with payment systems.

Let's call out that last one: if payment system data is at issue, *you should immediately locate and review your processing contracts* to see what they say about data breaches. Those contracts can raise issues that we won't go into here—the warning is that the contracts exist and many have express provisions and deadlines regarding data security breaches.

Okay, your attorneys have been called. What is the next step? It is one which might have led you to call your attorney in any case, *i.e.*, the implementation of a security breach response plan. If you have one, set it in motion.

Tip Re Your Plan: your incident probably won't be the result of an exotic "hack" into your online system. More typically, it will be something else, such as a lost or stolen laptop, an errant employee, a well-meaning but mistaken employee, a network security lapse, a courier company's loss of a back-up tape, or a physical break-in and theft of computers from your offices or an employee's car trunk. Security breach incidents can result from odd circumstances. My "favorites" are the ones suffered by (1) the Utah Department of Motor vehicles when thieves used a *forklift* to break in and steal the office safe and computer equipment,² and (2) the U.S. Internal Revenue Service which had to alert taxpayers in 13 states that 30,000 estimated tax payments sent to a San Francisco post office box were ejected into San Francisco Bay during a traffic accident.³ In short, it is impossible to predict or prevent all security incidents so your plan needs to be flexible enough to accommodate a variety of possibilities.

Preliminary Questions

If you have one, your security breach response plan will require you to gather basic information about the incident in order to know what to do from a legal and business perspective (which will be different than the technological steps your IT folks will be taking). As noted, numerous state and federal laws or private contracts or rules require notice of certain data security breach events; failure to comply can be costly in terms of fines, possible state and federal enforcement actions, private lawsuits, payment system liabilities and increased fees or audits, damage to reputation, loss of stock value, customer dissatisfaction and so on.

You won't be able to comply with these laws until you get enough information to determine whether they apply.

The data breach notice laws might not apply and you should not assume that giving notice is always "good" for the data subject and, thus, that you should launch the notice rocket immediately. Some companies have experienced an increase in attacks when word of notice indicated a vulnerability in their system, and notice recipients can be contacted by scam artists posing as regulators, company representatives or others purporting to need information in order to "help" the recipient "fix" the incident.⁴ Some regulators recognize this

and urge a measured approach. On the other hand, notice should not be withheld simply because you fear a loss of reputation. The point is that there are new laws in this area and they need to be examined in light of your incident to determine whether they apply.

The following questions are intended to help you do that. The answers are necessary to identifying appropriate next steps as a legal matter. When you get the "we've had a security breach" call, at least ask these questions. Also, *pin this article to your bulletin board* or pajamas (for those inevitable middle of the night calls)—you'll be glad that you did when you get the call.

1. When did the incident occur?

(Relevant to timing of required notices and determination of applicability of laws, including laws with delayed effective dates).

2. In what capacity was your company holding the data (e.g., was it holding it for another business and if so, what does that other business' privacy policy say about security breaches)?

(Statutory obligations shift depending on whether your company owns or licenses the data, or is processing or otherwise holding it for a third party owner. Any contract with another business needs to be reviewed).

3. How did the incident occur (lost or stolen computer, network breach, unauthorized access, etc.)?

(Relevant to (a) statutory coverage, (b) what types of other agreements might be relevant such as third party service agreements, employment agreements, etc., and (c) whether others might be liable to your company). Note: what you can learn about the incident by the end of a short statutory deadline for notice may turn out to be incorrect once the dust settles, so leave room for that possibility in any notice you must give.

4. What types of data were taken, accessed or exposed?

(Relevant to whether the event is covered under a payment system contract or a breach notification or other statute—each regime has its own definition of covered information and the range is wide and non-uniform. This question is also relevant to the statutory coverage question (*e.g.*, personal information held by the Veteran's Administration now has its own definition of "personal information" and its own notice rule⁵).

5. How many individuals are potentially affected and who are they (e.g., employees? customers?)

(Relevant to "materiality" for purposes of some statutes and also to formulating how best to deal with the incident—*e.g.*, if a large number of individuals will be

calling you, would an online facility or 1-800 number better handle the volume)?

6. What are the state(s) and countries of residence of the data subjects?

(Relevant to determining what law applies. The notice laws purport to pertain to data you have on a resident of the jurisdiction with the statute, even if the breach doesn't occur there and even if you have no presence there. This may create issues under international laws and, domestically, under the U.S. Dormant Commerce Clause).

7. Where do you do business?

(Relevant to statutory coverage question and the Dormant Commerce Clause issue—some of the state statutes do condition coverage on doing business in that state).

8. Is your company in a regulated industry (e.g., financial, healthcare, telecom), a federal agency, a contractor for a federal agency, or a service provider to a regulated entity?

(Special laws might apply instead of or in addition to state data breach notice laws).

9. Are there non-statutory requirements (e.g., payment system contracts or industry standards)?

(There may be notice or other requirements even if no statute applies).

10. Is your company publicly traded?

(Securities law reporting issues may need to be considered).

11. Was the data encrypted, redacted or otherwise rendered unreadable?

(Some statutes exclude from notice requirements some of such data).

12. Has the incident been reported to any law enforcement officials? What is the status of the investigation?

(Most of the statutes permit coordination with an investigation).

13. Has the incident been reported to anyone else (e.g., regulator or a payment processor)?

(Some statutes require notice to a regulator or other authority, and some contracts require notices (e.g., payment system contracts)—all under varying conditions as specified in the relevant requirement. Some of these notices must be given in as little as one hour among agencies. Sometimes reports must also be filed (e.g., "Suspicious Activity Report" for certain regulated financial institutions). Internally, senior officers

and public relations personnel should be brought into the loop.

14. Does your company have an external privacy or information security policy (e.g., for customers)? Do your attorneys have a current copy?

(Most of the state statutes allow an information policy – usually part of a privacy policy—to provide for how notice will be given).

15. Does your company have an internal privacy or information security policy (e.g., for employees)?

(Internal employment policies might trigger termination or discipline procedures).

Once you get answers your attorneys can begin to determine what laws apply—you will need to supply copies of your relevant contracts and there will be lots of additional questions, but answers to the above will at least get the ball rolling. If you are required to provide a notice, another important consideration will be the notice itself. At least one study indicates that the tenor and thoughtfulness of the notice are important components of the recipient's satisfaction with the company sending the notice.

In a perfect world perfect security would exist and all of this could be avoided. But it does not exist, no matter what precautions you take, so keep this list handy.

Endnotes

- ¹ See *e.g.*, Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer, 70 Fed. Reg. at 15736, 15752 (3/29/05)(under the guidance, a component of a response program is: "Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence[13] [13] See FFIEC Information Technology Examination Handbook, Information Security Booklet, Dec. 2002, pp. 68–74").
- ² See "Unlicensed Fraud: How Bribery and Lax Security at State Motor Vehicle Offices Nationwide Lead to Identity Theft and Illegal Driver's Licenses," Center for Democracy & Technology (1/04).
- ³ According to a 9/23/05 article, a contract courier was delivering mail from the post office to a check-processing facility when the accident occurred.
- ⁴ See *e.g.*, Raymond Nimmer and Holly K. Towle, *The Law of Electronic Commercial Transactions* (2003-2006, A.S. Pratt & Sons), at Chap.16.08[3](a)(sample phishing email from scam artist seeking information based on data security breach event).
- ⁵ See Title IX of The Veterans Benefits, Health Care, and Information Technology Act of 2006.