I. Introduction

Data breaches have become an unfortunate reality for many of the world’s largest companies. U.S. companies facing a data breach are currently left to deal with a patchwork of state and federal laws addressing data breach notification obligations. As of this writing, 47 states have enacted laws and regulations requiring private entities to notify affected individuals and state regulators in the event of a data breach (the remaining holdouts being Alabama, New Mexico, and South Dakota). At the federal level, there are also industry-specific breach laws, such as those for health care and financial service providers, that require notice to impacted individuals and government entities. Given the proliferation of high profile breach incidents, the federal government is working to enact a general data breach notification law applicable across industries, but it is unclear when that will occur and what impact it will have on the existing state data breach notification landscape.

Unfortunately for companies that experience a breach incident, notification may only be the beginning. Indeed, companies face potential costly exposure to federal and state regulatory action. For instance, in October 2014 the FCC levied a $10 million dollar fine against companies TerraCom and Your Tel America for not properly securing information for over 300,000 customers. In the Matter of TerraCom, Inc. and YourTel America, Inc., FCC Order 14-173 (Oct. 24, 2014). Companies may also face expensive class action litigation stemming from the breach. For example, in June 2014 Sony agreed to pay up to $19 million dollars to settle litigation alleging that it failed to provide reasonable network security to protect user information. In re Sony Gaming Networks and Customer Data Security Breach Litigation, No. 11-md-2258 AJB (MDD). And data breaches may have long lasting effects. In October 2014, a Louisiana state court approved a $32.5 million dollar settlement by Tenet Healthcare for disclosure of

---

1 Adapted and updated by the Internet/Privacy Subcommittee from Providing Notice After a Data Breach – The Top Ten Steps, by Liisa Thomas, Monique Bhargava, and Robert Newman, Winston & Strawn LLP (2014), with permission.

Even aside from regulators and legal action, the costs of investigating and remedying any breach may be staggering. For instance, in December 2013 online thieves stole credit card information and personal data from Target’s computer system. The company estimates that it has already spent $148 million to investigate and remedy the breach and to offer a year of free credit screening for customers who believed their data had been stolen. Thinking about this exposure before providing notice, and when investigating a potential breach, is thus quite important.

II. Key Considerations

Harmonizing the various applicable laws and legal theories under which an action a may be brought is beyond the scope of this Core Knowledge article, but the following list describes key general themes that all attorneys should keep in mind when advising clients that might be facing a data breach.

A. Evaluate what breach notice laws govern your company.

Even if a business is only located in one state, the state breach laws will likely apply based on where the business’ customers reside. Consequently, if there is a breach involving customers in all fifty states, the business will arguably be subject to breach notification laws in almost every state.

Additional state and federal laws govern certain types of entities. For example, financial institutions and service providers may have notice obligations under Gramm-Leach-Bliley Act (“GLBA”), and covered entities and their business associates have breach notice obligations under the Health Insurance Portability and Accountability Act. There are also (a growing number of) foreign jurisdictions that require notification in the event of a data breach.
A company may also have certain contractual obligations to provide notice to certain providers. Examples include obligations placed on companies that offer mortgages under Freddie Mac or Fannie Mae or businesses that accept credit cards or are otherwise subject to PCI obligations.

**B. Identify what information may have been subject the incident**

Not all personal information, if compromised, triggers laws that require notification. Most laws require notice only if certain sensitive information has been compromised (financial account information, government issued IDs, social security numbers, etc.). However, several states have broader categories of triggering information. For example, California and Florida’s breach notice laws were amended in 2014 to include as triggering a user name or email address combined with a password. Some laws are triggered by very unique items, such as North Dakota which requires notification if name and date of birth has been breached.

**C. Determine whether the incident constitutes a “breach.”**

At the heart of determining whether notification is required under the relevant laws is to analyze the incident itself, and whether it is viewed as a “breach.” While the definition of breach varies, there are typically two factors to analyze: (1) whether there was unauthorized access or acquisition of triggering information and (2) if the integrity, confidentiality, or security of the triggering information was compromised. Many laws contemplate that companies will (or must) conduct investigations or work with law enforcement to determine what happened in the incident.

**D. Analyze if there are any applicable exceptions to notification**

Even in instances where an incident might otherwise fall within the legal definition of a “breach,” an exception may still apply that would keep a notification obligation from triggering. For example, if information was encrypted, or if the access or acquisition was made in good faith by an employee or agent, and the information was not otherwise put at risk.
In some jurisdictions, there are exceptions to following the state law for entities that are required to follow other breach notification regulations (like the notification regulations under HIPAA or GLBA). Even if notification is not required, a company may still want to consider providing it to ward off a regulator or class action argument that the company did not give individuals information they could have used to protect themselves.

**E. Identify who needs to receive notice**

Data breach notification laws require notification to affected individuals. Many also require notification to regulators, such as states’ attorney general or an industry-specific regulator. Some state data breach notification laws also require notice to credit reporting agencies. Whether to notify regulators or credit reporting agencies is often dependent on how many impacted individuals there were. If notice is required, companies would be well served to look at contractual obligations as well. For example, as noted above, companies that accept credit cards as payment will have obligations under the PCI Standards, or those that issue mortgages backed by Fannie Mae and Freddie Mac will need to notify those entities.

Note that even though these laws require notification to affected individuals, the business may not be the entity required to make that notification. Some states, like Arizona, and Delaware, require that the notice to individuals is provided by the entity that “owns or licenses” the data that may have been breached. In those instances, if a company maintains or uses the data but does not own or license it, obligations may be limited to providing notice to and sharing information concerning the breach with the owner or licensee. In all events, you may decide to handle the notification anyway depending on your relationship (contract or otherwise) with the owner or licensee of the data, the number of potential individuals who must be notified, and whether and to what extent your insurance policy covers the handling of a data breach.

Keep in mind that state laws generally do not require notification where the impacted information was “encrypted.” Consequently, businesses should be encouraged to encrypt personal information where possible.
**F. Determine what needs to go into the notice.**

In some jurisdictions, if notice is required, there is very specific content that needs to be included in the notice. Required content can include things like describing the breach and the type of information compromised, remedial actions a company has taken, steps an individual should take to protect him or herself, and contact information for the company, state regulators and for the Federal Trade Commission. Keep in mind that some states actually prohibit certain information. For example, Massachusetts does not permit inclusion of the nature of the breach, and neither Massachusetts nor Illinois permit including the number of affected individuals.

Also keep in mind that some companies will provide identity theft monitoring to those whose data has potentially been breached as an act of good faith to avert potential issues with the use of the data, and in an effort to discourage action by the individual; in fact, a California law that went into effect on January 1, 2015 arguably requires the provision of such services for certain types of breaches. Some insurers will provide coverage for this use. Check your insurance policy to see if you have coverage, and if so, what requirements you must meet to obtain the maximum.

**G. Decide how and when to provide notice.**

Most regulations contemplate sending notice to impacted individuals by mail, although some permit email or phone notice. In some cases, a company may not have contact information, or may have too many people to notify. In those circumstances it will want to think about providing “substitute” notice, which is permissible under many laws if thresholds are met (e.g., cost to notify, impacted individuals). Substitute notice typically requires that a business give notice be by all of the following: (1) email; (2) conspicuous posting on the company website; and (3) notice to statewide media.

In the U.S., notice to individuals is typically required to be made without undue delay or as quickly as possible. Outside of the U.S., some jurisdictions contemplated almost instantaneous notice (after one or two days). Notice to regulators — where required — may also be subject to
timing requirements.

**H. Prepare a public relations strategy.**

Once notification to consumers and regulators is made, the data breach has been made public. This is when the public relations risks come into play, and the prepared company is one that has thought about its PR strategy before notice is sent. Think about the type of questions that might be asked, and have responses ready. Common questions include whether information was encrypted, what the company is doing to protect individuals, why the company waited to notify (even if the “wait” was only a few days), whether a similar incident is likely to occur again, and the most common question: “is this notice a hoax?”

**I. Draft a response for regulator follow-up.**

In addition to responding to consumer and media inquiries, companies should be prepared to respond to inquiries from regulators. Depending on the nature and extent of the breach, regulators may initiate investigations to determine what security protocols were in place at the time of the breach and what steps the company has taken to prevent similar data breaches in the future.

Some inquiries may be relatively straightforward, an exercise to confirm facts and clarify the items contained within the notice. However, other inquiries can be extensive and intrusive as regulators attempt to determine if a company has complied not only with the data breach notification laws but also with general data security and trade practices laws which may — at least in the eyes of the regulators — place obligations on the company to adequately safeguard personally identifiable information.

**J. Prepare class action defense strategies.**

Unfortunately, a data breach often leads to class action litigation. However, these cases are not always successful and there are important defenses that should be considered. For example, a
number of class actions that have arisen in the data breach context have been dismissed for lack of Article III standing due to a lack of harm to the plaintiffs. For example, in Ohio, a class complaint filed after a breach of Nationwide Mutual Insurance was dismissed where the plaintiffs failed to adequately allege that their personal information was actually misused as a result of the breach. Applying the Supreme Court’s decision in *Clapper v. Amnesty International*, in which the Supreme Court held that a “theory of future injury is too speculative to satisfy the well-established requirement that threatened injury must be ‘certainly impending,’” the district court held the risk of identity theft is not “certainly impending” because its occurrence depends on the decisions of independent actors.

**K. Evaluate steps to address vulnerabilities and prevent another breach.**

Throughout the investigation stage, a company will learn that it could have taken protection measures and implemented practices that might have prevented a particular incident. Regulators and individuals alike will ask if these steps have been taken. There is an expectation that companies will address known security issues promptly in the wake of a data breach. Failure to take further steps to prevent future breaches can also expose companies to additional unfair and deceptive claims in the event of a subsequent data breach.