Data Breach Incident Response: 5 Questions to Ask and New Laws to Know Now

07.11.2016 | UPDATES

The spring legislative sessions this year brought a now-familiar round of revisions to data breach notification laws, with states broadening their laws in often divergent ways. This year, Illinois, Nebraska, and Tennessee passed revised laws, and laws passed by Nevada and Rhode Island last year are just now coming into effect. The changes arise alongside the added complication of two decisions from the U.S. Court of Appeals for the Seventh Circuit that rely in part on the content of data breach notifications. These new laws and precedents continue to complicate best practices for responding to an incident compromising personal information.

From whether a reportable breach has occurred, to when and how to notify affected individuals, companies responding to a potential data breach should carefully consider the traditional questions of incident response in light of these new developments.

1. Is it a reportable breach? The types of personal information that trigger data breach notification requirements continue to grow beyond the traditional list of social security number, driver's license number and financial account numbers. This year, Illinois and Nebraska (as well as laws in Nevada and Rhode Island passed last year but effective this month) continue the trend of adding online account credentials to the definition of triggering personal information, requiring many companies that otherwise collect limited personal data to consider these issues. (These states join California, Florida, and Wyoming in requiring notification for compromised account credentials.) Illinois and Rhode Island also added medical and health insurance data to their statutes, while Illinois joins six other states that include biometric data.

Typically, unauthorized access to personal information only triggers notification if the information is unencrypted, but this year, Tennessee removed the explicit mention of encryption from its statute, intending to remove that safe harbor. Rhode Island also now specifies that "'encrypted' means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process." As a result, companies that lose encrypted personal information must assess the type of encryption applied and whether the loss is likely to compromise the "security, confidentially, or integrity of the data." Weak encryption may no longer meet state standards.

2. How fast should you notify? Data breach statutes traditionally require only that notifications be made "in the most expedient time possible," with no express deadline. In recent years, however, states have begun putting outer limits on what a "reasonable" time period might be, most commonly 45 days after discovery of the breach. This year, Tennessee and Rhode Island joined this bandwagon in requiring notification within 45 days.

Statutes notwithstanding, many companies seek to announce a breach as quickly as possible to appear responsive and protect their customers. Moreover, courts have indicated that claims based on delayed notice could be viable if plaintiffs can show the delay caused them injury (although no plaintiffs have actually successfully done so).

The recent *Lewert v. P.F. Chang's* decision from the Seventh Circuit should give companies pause, however, particularly those considering publicizing an incident before all the facts are known. When P.F. Chang's discovered a breach in their payment systems in June 2014, they quickly took the system offline nationwide, publicly announced a breach of unknown scope, and urged customers to be cautious. They discovered within a week that the breach affected only a handful of restaurants. In response to a suit from its customers, P.F. Chang's claimed that customers of other restaurants not affected by the incident did not have their data stolen. The court rejected this argument, citing P.F. Chang's early notice that warned *all* their customers that they were at risk. While leaving open the possibility that discovery might eventually show that plaintiffs were not in fact harmed by the breach, the court denied P.F. Chang's motion to dismiss and allowed the case to proceed.

In light of this analysis, companies should carefully consider public announcement of an incident when the facts are unclear, weighing potential risks to customers against unintentionally increasing the worry and concern that may translate into expanded legal action.

3. What should the notice look like? States continue to tinker with the content of legally required data breach notifications. Rhode Island's new law contains six specific requirements in a combination that will likely require a unique form of letter be used in Rhode Island (or, at the very least, substantive changes to the type of letter that was previously compliant in all states except Massachusetts).

Rhode Island, like other states specifying notice content, dictates standard content regardless of the type of incident or information at issue, but this required language can cause problems in later litigation. For example, the court in *Remijas v. Neiman Marcus* discounted Neiman Marcus's assertion that only credit card information was involved—and not information that could be used to open new credit accounts—because it stated in its notice, *as it was legally required to in several states*, that affected consumers should check their credit reports.

This analysis suggests that companies should think carefully about how to meet state requirements regarding the content of notice without creating additional litigation risk.

4. Who receives notice? All state breach notification laws require that companies notify the individuals affected. A growing number of states also require companies to notify the state's attorney general or a related office. Nebraska and Illinois (for state agencies only) joined the list this year, following Rhode Island, Montana, North Dakota, Oregon and Washington last year. In addition, states continue to roll out their own customized forms for attorney general notification, further increasing the effort required to comply with nationwide notice requirements.

5. Should you offer credit monitoring? Victim companies commonly offer credit monitoring in large, high-profile breaches. Since 2015, Connecticut has required credit monitoring for breaches involving social security numbers. (California, and now Rhode Island, also require that the services be described in the notice *if* they are offered.) Many companies also offer credit monitoring and identity theft restoration services even when only payment card information is potentially compromised. Credit monitoring will not detect misuse of payment cards, and payment card numbers cannot be used to open new accounts that monitoring will detect, but the offer is widely considered to provide a measure of comfort to affected individuals and to be in line with expectations set by large breaches like Target and Home Depot.

But companies should also be aware that the offer can come back to haunt the company in litigation. The court in *Remijas* cited the offer of credit monitoring (along with the reference to credit reports cited above) as evidence that Neiman Marcus believed there must be some risk to its consumers beyond credit card fraud. As a result, customers that claimed types of harms that do not arise from the theft of credit card information were nonetheless allowed to proceed in their suit.

Each of these laws has been incorporated into Perkins Coie's newly updated Security Breach Notification Chart.

In addition to increasingly divergent U.S. laws, both Canada and the European Union are in the process of releasing new data breach notification regimes that companies operating internationally will need to consider as well. Companies holding personal information should carefully assess their incident response procedures and breach notifications in light of these changes.

CONTACTS

Amelia M. Gerlicher
Counsel
Seattle
D +1.206.359.3445

Todd M. Hinnen
Partner
Seattle
D +1.206.359.3384

Related Services

- Privacy & Security Law
- Internet & E-Commerce
- Retail & Consumer Products