Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Tips For Responding To A Mega-Sized Data Breach

Law360, New York (May 11, 2016, 5:56 PM ET) --


Brookes Taney

One of the largest issues impacting the business world today is information security. In recent years, the number of data breach incidents has skyrocketed, now commonplace in nearly every segment of the business world. Despite the efforts of companies and government agencies to protect sensitive data, larger and more complex data breaches continue to hit the headlines. In 2015, 38 percent more security incidents were detected than in 2014, according to PricewaterhouseCoopers' survey "The Global State of Information Security." Today, companies are grappling with how to react quickly to the growing onslaught of breach incidents while also trying to stay one step ahead of the next attack.


Stephanie Fiereck

All too often, companies find themselves unprepared to respond to the complexities of a breach, especially a large or mega-sized data breach.[1] It can be difficult for companies to manage the sheer volume of data involved, not to mention all the logistics associated with handling the massive number of calls in response to notice of a breach. This article will provide a framework of effective strategies for how to handle these issues and comply with regulatory notice requirements when responding to a mega-sized data breach incident.

Reigning in the Data: Timing Is Everything

Prompt investigation is essential once a company determines that an incident occurred. In addition to the challenge of identifying what data was actually compromised, one of the most difficult aspects of responding to a mega-sized data breach is compiling all the data in preparation for providing notice to those affected. It sounds simple, but with a data breach, the first priority is to identify the scope, determine the data impacted and identify who needs to receive notice.

There can be millions of records from numerous sources, including servers, file shares, third-party databases and so on. Many organizations find it difficult to ensure all the possible sources of data have been identified while the full scope of the breach is often still being determined. This is especially true when good data mapping is not in place. It is also challenging because once a breach is discovered, the clock starts ticking for providing notice to those impacted by the breach under various state and federal laws.

Although there may be a desire to wait as long as possible to supply data to a data breach notice provider, this can be problematic in a mega-sized data breach for a number of reasons. First, prior to

mailing a data breach notice, a data breach response team needs adequate time to compile all the data, standardize and normalize it, remove duplicate records and then run addresses against the U.S. Postal Service National Change of Address database in an effort to minimize the number of undeliverable mail pieces. In the recent enormous data breach impacting a large health plan company, nearly 40 million records in more than 25 files were combined and de-duplicated to fewer than 10 million records for the breach notice mailing. This effort to remove approximately 30 million records saved the company a small fortune in postage alone.

Second, allowing adequate time to prepare for the breach notice effort can provide an opportunity for the notice provider to do a test drop of the notice mailing. This allows the notice provider to gain insights into the potential response of those affected and make predictions for purposes of planning for the number of call center agents needed, etc. This can be invaluable information. Finally, if time allows, it can be advantageous to schedule the notice mailing so it is staggered over a number of days, rather than all the notices going out on the same day. This can help avoid a massive response to both a dedicated breach call center and to a company's internal phone lines, which can be difficult to prepare for and respond to properly. For these reasons, companies are typically well served to compile all the necessary data as soon as possible and provide it to the data breach notice provider. Ideally, providing the data to the notice response team one to two weeks prior to the notice mailing deadline will maximize the results and cost savings.

Providing Notice

There are a number of considerations that are important when providing notice of a mega-sized data breach incident. For example, when drafting the notice text, a clear and easy-to-understand notice with non-alarming content tends to generate the best response and result in fewer calls and shorter call times, which can be a huge cost savings with a large breach. Also, try to limit the number of unique notice templates drafted. Five to 10 different notice types is ideal for most data breach notice efforts. In cases where additional unique notices are necessary, allow ample time to compile the various notice documents.

In a recent breach that involved a large health plan company, the response notice effort was massive with approximately 300 unique notice templates to provide state and federal mandated notice of the breach. This required substantial lead time to update and proof the hundreds of notice templates to ensure everything was accurate prior to mailing millions of notices. A large number of unique notice templates will likely increase the cost of administration, increase the risk of potential errors within the notices and put a strain on already tight timelines.

Preparing for Callers: Customer Service is Everything

The one aspect of responding to a mega-sized data breach that can be particularly trying for most companies is putting together a call center quickly amid handling all the other aspects of the breach. The challenge is simple: How do you set up a call center with 500 or more agents trained and ready to handle an onslaught of calls in a matter of days?

For a large data breach, a quick turnaround for setting up the call center is critical due to the extremely short timeline. Phone scripts, agent training materials and answers to frequently asked questions need to be drafted and approved. The interactive voice response system routing needs to be planned, programmed and routing and hold messages need to be drafted, approved and recorded. In addition, potentially hundreds of call center agents must be hired and trained. The level of training provided to

agents is important. Agents need to be prepared to handle a whole spectrum of callers, especially those who are upset, confused and impatient. The better the training, the quicker agents can calm callers and answer questions by providing good customer service. This is important from a crisis management and brand perspective for the breached company.

The secret to success is good customer service and short caller wait times. Answering calls within 30 seconds to one minute is ideal. Longer wait times result in unhappy callers. Class actions are more likely to occur when already frustrated consumers sit on hold for long periods of time attempting to get information regarding a breach. The focus should be on serving those callers and addressing their concerns. Callers must come away from the conversation feeling that their complaints have been heard and that the situation is under control.

Know the Target Audience

When providing notice to consumers, consider using an online web enrollment in addition to a call center. Consumer adults aged 18-60 prefer to enroll for credit monitoring services, etc. online rather than via other forms of communication. Whereas if the target audience are senior citizens they generally prefer to call a toll-free number to speak with a live operator to enroll and generally require longer call times. Another consideration is data breach fatigue, particularly when providing notice of a data breach in consumer cases. Consumers have been inundated by the media and the constant coverage of the data breach epidemic and as a result their response to notice of consumer related data breach incidents has declined. As a result, it is particularly important that breach notices be clear and concise to provide consumers with quick and easy direction in order to respond to a breach.

Conclusion

Incidents of data breach will likely remain a strain on businesses. Regardless of the circumstances of a given data breach incident, how companies respond to the breach is critical. By being prepared to handle the challenges of responding to a mega-sized data breach, companies can be better equipped and possibly avoid future class action litigation. All this adds up to reduced risk and cost when handling large data breaches, so companies can get back to business.

—By Brookes Taney and Stephanie Fiereck, Epiq Systems Inc.

Brookes Taney is a vice president of data breach solutions and Stephanie Fiereck is a manager of legal notice at Epiq.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] While there is no industry-standard terminology to characterize the size of a data breach, in the context of this article, a large or mega-sized breach is one with a half million to a million or more individual records impacted.