Communicating a data breach

Experian Data Quality

Data breaches present a real problem for businesses, and the frequency of these incidents is on the rise. A 2012 survey by the National Cyber Security Alliance and McAfee found that one in four Americans had been officially notified that key elements of their personal information had been lost. With major data breaches dominating the news already several times in 2014, this topic will continue to be a focus and companies.

There are a host of steps that should be completed to prevent data breaches, but companies should also prioritize creating a crisis plan. In the event of a large-scale breach of personal data, companies need to be prepared to act quickly to minimize the damage that data theft poses to the company, its reputation and its customers.

One of the critical components of this crisis plan is communication. Early notification to affected individuals gives them the ability to cancel any credit cards or details before criminals can cause real damage. In addition, it can help the company mitigate any brand image damage and loss of revenue.

However, planning is key. Organizations need to understand the requirements for communication and data quality challenges that are commonly faced when dealing with a data breach.

Requirements for communication:

Certain data breaches require businesses to notify customers. At least 46 states, the District of Columbia, Puerto Rico and the Virgin Islands have laws requiring notification of data breaches.

Typically, this notification must take place when a piece of personally identifiable information (PII) is tied with either an account number, credit card number or social security number.

During a notification event, businesses need to work to communicate quickly with customers. Certain states have time frames in which you are required to notify customers, some within 30 days. These communications need to include toll-free numbers and postal addresses for:

- The three major credit bureaus
- The FTC
- The State attorney general

Multiple states laws may apply to one data breach because the jurisdictions depends on where the affected individuals reside, not where the business is located. If some individuals live in a state that mandates notification and others live in a state that doesn't, everyone should still be notified so companies are not targeted for inequality.

A two-pronged communication approach:

In the event of a data breach, it is important to notify all customers as quickly as possible. There are traditionally two primary forms of communication used: email and physical mail.

As a best practice, companies should look to utilize both channels. Some states require written notification via physical mail, but obviously the process can take more time to execute. To notify customers as quickly as possible, email is best.

This two-step approach will help ensure written communication requirements are met across the various states with affected customers and that customers are notified quickly enough to secure their own information.

Data validation is a must:

Before communications are sent, be sure your contact data for customers is up to date. On average, US companies believe 25 percent of their data is inaccurate. That means that without proper verification and correction, you may be unable to communicate with a quarter of your customer base in the event of an incident. Not only does this harm your customers, but it also exposes your business to compliance gaps.

To ensure that as many emails as possible can be delivered to the inbox, companies should utilize email validation to identify and remove invalid email addresses. This is especially important when emailing sections of the database that may not be actively engaged in marketing programs or email communications. Most often, this segment contains outdated information or invalid emails. By sending to these addresses, your organization can expect higher-than-average bounce rates and could be blacklisted, impacting your ability to reach the inbox. This will affect data breach communications, but also any marketing or operational communications you may want to send in the future.

For mailing addresses, be sure to verify physical addresses to make certain the data is accurate and complies with USPS® standards. Poor address data quality can lead to returned mail and delays on mandatory written communications. This can leave companies out of compliance based on regulatory deadlines.

In addition to identifying and removing invalid data, companies can utilize data quality software to create more targeted communication plans for those customers who do not have accurate contact information on file. Communication gaps can be addressed immediately by collecting accurate information or utilizing other communication channels.

Conclusion:

With data breaches increasing and criminals becoming ever more determined, it is important for companies to have a strong plan in place for a potential breach. Communication is an important component and companies should validate the accuracy of customer contact data to ensure the delivery of communications. A strong communication plan will help protect customers, but also help your company mitigate any brand image damage and loss of revenue.

Experian® Data Quality

About Experian Data Quality

Experian Data Quality is a global leader in providing data quality software and services to organizations of all sizes. We help our clients to proactively manage the quality of their data through world class validation, matching, enrichment and profiling capabilities. With flexible SaaS and on-premise deployment models, Experian Data Quality software allows organizations around the world to truly connect with their customers by delivering intelligent interactions, every time.

Established in 1990 with offices throughout the United States, Europe and Asia Pacific, Experian Data Quality has more than 13,500 clients worldwide in retail, finance, education, insurance, government, healthcare and other sectors. For more information, visit http://www.qas.com.