SpencerFane®

# Data Breach: Are You Prepared to Respond?

**NOVEMBER 17, 2014| PUBLICATIONS**

Data breaches are becoming an everyday occurrence. Just ask The Home Depot, Target and Schnuck's. The number of companies reporting a data breach increased over 30% in the past two years. Experts agree that every company is susceptible to data breaches, and that it is not a question of if but when it will happen. Banks are especially vulnerable because of their unique position as both a target themselves—for the goldmine of personal and financial information they control—and their connection to virtually every consumer and business in the country. When an individual suffers a breach, it often includes financial information like bank accounts and payment cards. When a business suffers a breach, the business's financial accounts may be compromised along with its customers. In either situation, consumers look to banks to react quickly to mitigate the damage even though the banks were not at fault. A mismanaged data breach response threatens your relationship with customers.

Data Breach Response: What is Required

Missouri, like many other states, has enacted data breach notification laws. These laws are intended to ensure that consumers are informed of incidents that risk exposure of their personal information. Missouri's law is no different, requiring notification when unauthorized access to or acquisition of personal information creates a "reasonable likelihood of harm." This notification, at a minimum, cannot be "unreasonably delayed" and must include a general description of the breach, the type of information that was exposed, a telephone number that consumers may call, consumer reporting agency contact information, and a recommendation to monitor financial accounts and credit reports. For large breaches, affecting over one thousand consumers, notification to the attorney general and consumer reporting agencies is also required.

Data Breach Response: Best Practices

Earlier this year, the ICBA released a guide – *Key Considerations for Community Banks Facing Payment Card Compromises* – addressing issues that banks need to consider whenever responding to a data breach event. First, assess the situation and the scope of the breach. Banks need to assess the situation by reviewing fraud alerts from its payment card network to help answer questions, such as which customers and what information was compromised. Second, decide whether to reissue payment cards. Depending on the assessment, the breach may have compromised card numbers warranting new cards to be issued. Third, communicate the breach to effected customers. Customers expect timely notification of suspected breaches, preferably within 24 hours. Communications should describe the breach in sufficient detail to inform the customer of how the breach occurred, what information was exposed, and what steps the bank is taking to protect their information, including the reissuance of cards if necessary. Additionally, the communication should reassure customers that the bank takes their security seriously and that they have zero liability for fraudulent activity (if applicable), and remind them to monitor their accounts for any unauthorized transactions.

Be Proactive

Banks should create a data breach response plan to proactively prepare for a data breach event. The plan should identify procedures for assessing the scope of the breach and designate roles to employees responsible for responding to a breach. The assignment of roles helps to ensure that a clear and focused message is communicated to customers and the media.


**AUTHORS**

- Jonathan R. Gray


**BLOG TOPICS**

- Community Bank Counselors
- Privacy and Cybersecurity Solutions

Banks are expected to act expeditiously to mitigate potential harm and communicate with its customers even when the data breach was caused by a retailer. Customers provide personal information to banks with the expectation that it will be protected. This confidence can be shaken when a breach occurs. A bank with a data breach response plan can restore confidence by responding appropriately and quickly.