AMERICAN BANKER

How Not to Handle a Data Breach

by Penny Crosman
OCT 7, 2014 1:19pm ET

There's almost no good way to tell bank customers that their personal data has been stolen. But some banks do a particularly bad job of communicating during a security incident.

Example: one consumer came home last week to find a voicemail from his bank (one of the top five) telling him his account had been compromised by a "midsize retailer breach." The message raised more questions than it answered. What was midsized — the retailer or the breach? What information was stolen? What was he supposed to do about it? The consumer was left confused and fretful.

"I've heard other such examples of robo-dialer notifications in the wake of a breach that are even more unsettling from the consumer's perspective," said Julie Conroy, research director at Aite Group. In some botched robo-calls, Conroy said, the voicemail has picked only up the latter half of a canned, impersonal recording. The consumer didn't know who was calling or which card was breached, only that there was a problem somewhere to investigate.

Communication strategies for data breaches are as important as they have ever been. Last week, JPMorgan Chase disclosed that names, addresses, phone numbers and email addresses for 76 million customer households and 7 million small business clients had been compromised. Regulators are paying closer attention to cybersecurity; earlier this

year, the Federal Financial Institutions Examination Council announced plans to conduct cybersecurity exams of banks. And the sheer volume of data breaches over the past twelve months has been staggering: according to the Ponemon Institute, 43% of U.S. organizations have suffered a breach in the past year.

A breach is not something a bank should sugarcoat, obfuscate or ignore, especially considering the lightning-fast speed at which the news will travel through social media and news outlets.

It's important for key customers and stakeholders to hear the news about a breach first from the bank directly, and not through the media, said Dwayne Melancon, chief technology officer of Tripwire, a security and compliance software provider. "This isn't always possible, but it is an important goal to strive for."

But while they need to react quickly, banks clearly need to be careful about robo-calling.

"For large national banks, automation is inevitable, but the automation process and the message communicated should be well-thought through and tested to ensure it doesn't create more concerns than it is addressing," Conroy said.

Banks faced a similar challenge during the large distributed denial of service attacks against their websites in the fall of 2012, Conroy pointed out.

"Some of the early banks affected did not provide customers with clear communication on what was happening, assurances that their money was safe, and what their alternatives were," she said.

Banks also need to establish spokespeople for social media and press relations. "It is important to maintain consistency in the external messages to avoid confusion and reduce the risk of unproductive speculation," Melancon said. "Being consistent and deliberate in the external messages you convey is extremely important."

There are myriad legal rules that govern what banks can and cannot say during and after a breach of customer data. The Gramm Leach Bliley Act asks banks to think about what the impact on their customers might be. A breach of private information, such as Social Security and credit card numbers, obviously has a bigger impact than the compromise of public information such as telephone numbers or addresses.

In JPMorgan Chase's case, the customer data included addresses, phone numbers and email addresses. This is all information that can be easily found on the Internet. But combined with the knowledge that the person is a Chase customer, it is ideal fodder for phishing. The bank has warned its customers to be on the lookout for suspicious emails.

There are also 47 state laws that guide banks on notification during data breaches. National and regional banks have to comply with multiple laws per breach.

Another factor that has to be taken into account is the law enforcement considerations and national security implications. For instance, if there's reason to believe the attack might have come from a nation-state, the FBI or Department of Homeland Security may set the communications rules. In such cases, banks are often asked to keep things under wraps for a while until the authorities investigate.

"In the same way that you don't want to tip a robber you're about to rush them, you don't want to tip the cyber actor that you're about to catch them," said Paul Smocer, president of BITS, the technology policy division of the Financial Services Roundtable trade group. "There are provisions in the law that allow law enforcement to do 30-day deferrals on notification."

Well-prepared companies prepare for a breach before they ever get hit, Smocer said.

"Best-in-class organizations have done a couple of things ahead of time: they've engaged people throughout the organization who will need to play a role in the event a breach occurs," he said.

And this doesn't just mean the IT staff.

"Of course the tech team has to be involved, but wise organizations will also have CEOs and other C-level managers engaged, product managers engaged such as the person in charge of credit cards," Smocer said. Online banking, mobile banking and call center managers need to be involved, as do marketing and public relations people and third parties, such as a credit monitoring provider that might need to provide a year of free monitoring for victims.

"You need to think about who's going to speak with your constituencies, law enforcement, customers, the media," Smocer said. "You almost have to lay out a plan that covers reasonable scenarios: what happens if we're breached and private customer information is stolen, if intellectual property is stolen, if the third party we work with is breached and our customers' information is affected. You need to assemble the team, run through some scenarios you can reasonably expect."

There are also positive industry role models for dealing with a data breach.

In the wake of the Target breach, one credit union's CEO called customers personally to notify them of the breach and walk them through next steps, Conroy recalls.

And as the DDoS attacks took place, PNC stood out for its deft communications work.

"PNC's response was excellent — they were very honest with customers about what had happened, they assured customers their data and money was safe, and they provided clear communication about alternate ways to engage with the bank," Conroy said.
