



HOW TO MAKE 'DEAR JOHN' DATA LETTERS MEANINGFUL

Posted: Friday, August 22 at 05:00 am CT by Bob Sullivan

I like to call them "Dear John" data letters. And just like those sad, cold notes from a lover announcing a breakup, those "We've lost your data" letters are almost always frustratingly vague.

A new study from identity theft research firm ID Analytics suggests that's both unfair and risky. The study shows that consumers victimized by insider data theft -- theft by an employee -- are 12 times more likely to be ultimately hit by fraud than victims of an accidental data loss, like a lost laptop computer.

Yet many Dear John data letters announcing security breaches offer precious few details about the circumstances of the loss. That leaves consumers completely in the dark about what to do.

While data leaks rarely make headlines now, as they've become frighteningly commonplace, the rate of leaks has steadily increased since 2005, when disclosure laws began forcing companies to fess up to them. About half of U.S. adults have received at least one such letter, according to the Ponemon Institute. And since 2005, more than 236 million pieces of data have been lost or stolen, according to the Privacy Rights Clearinghouse.

But data loss letters are often short on critical details, such as how the data was leaked or why. Such information provides important context to consumers and would help them determine how they should respond, said Mike Cook, co-founder of ID Analytics.

"Some of the letters I have seen have not been as informative as they could have been, which is a disservice to both consumers and businesses," Cook said.

Here's why the details matter. ID Analytics analyzed 5 million pieces of identity data stolen in 12 separate insider thefts. More than one-third of consumers exposed by those incidents -- 36 percent -- were ultimately hit by identity fraud. Contrast that with ID Analytics data on lost laptops and hard drives, where victims were hit with fraud only about 3 percent of the time.

"All data breaches are not created equal," Cook said. "It's important for consumers to understand that."

Make it a doozy

Other circumstances surrounding the breach also help predict the likelihood of fraud, Cook said. This might sound counterintuitive, but the findings suggest that the larger the data leak, the less likely a victim will be hit by fraud. Consumers who have their data stolen as part of a small, targeted incident -- say 10 identities copied by an insider -- are at greater risk than consumers who are exposed through a theft of 10 million credit cards.

"If I am a consumer, and I learn that I am part of the largest breach in history, I should be happy because the likelihood of my name being used at random is very low," Cook said. "But if I am part of an internal breach of 10 identities, I should be very concerned."

The three questions that should be answered

Consumers who are victims of data breaches should always get the answers to three critical questions, Cook said: the size of the breach, the precise data involved and the reason it was stolen or lost.

Those answers, however, are rarely forthcoming, said Gartner security researcher Avivah Litan. Many companies reveal almost nothing about a data leak, which prevents consumers from making common-sense decisions about how to react.

"The disclosure laws should be refined to give consumers this type of information," she said. "Right now these letters don't mean anything if there are no details. Consumers don't have enough information to make an educated decision about what to do."

The ID Analytics study comes at a time when Congress continues to debate a national data loss disclosure law. Currently most states require data loss disclosure, but a national law would likely supersede state laws.

Federal legislation favored by the credit industry and the Federal Trade Commission would limit disclosure to leaks when there is a great likelihood of actual fraud. That means lost laptop computers and hard drives might not trigger notices. But so far there has been little discussion of making companies offer more specifics to consumers when such disclosures are required.

It's about the intent, not the source

Alfred Huger, a researcher at security firm Symantec, said he suspects there isn't much difference between data stolen by an insider and data stolen by an outside hacker who is part of an organized crime gang. What matters most is the intent of the thief, he said.

"There are some collections of hackers who are quite precise about what they are going to steal and what they will do with the data," he said. Data stolen by such hackers is probably equally likely to result in fraud as data taken by determined insiders, he said.

But the ID Analytics study unearthed a few additional details about insider theft. In every case, the stolen data was used locally -- within 20 miles from the place of the theft, Cook said. That suggests the criminals were not part of complex international crime rings, he said.

"People are stealing the data and using it themselves, or giving it to someone they know," he said.

The report also revealed a sharp rise in mobile phone theft, with 69 percent of fake applications used to apply for a cell phone. That result follows a study earlier this year by ID Analytics that showed mobile phone theft now makes up 32 percent of all new account fraud, up from 19 percent just last year.

In the past, ID criminals routinely applied for cell phones so they'd have phone numbers to put on fraudulent applications for credit. But today, Cook said, given the rising cost of multi-function phones, criminals simply obtain discounted smart phones with two-year contracts and then sell them at high profits.

"Attacking mobile phones is a growing phenomenon," he said.

It's also a huge pain for consumers, who rarely find out about cell phones opened in their name unless they check their credit reports.

RED TAPE WRESTLING TIPS

Given the continued avalanche of data breaches and data loss letters, it is understandable that legislators might want to limit the notices to those that matter most -- those incidents where risk is ID theft is high. This would mean companies that lose laptops and hard drives accidentally would probably get a free pass. That's an undesirable result, as the public shaming of poor security practices has helped bring focus to the twin issues of privacy and data security.

If consumers are to lose the right to know every time a company loses track of their data, they should get something in return. Firms should be forced to offer far more explicit detail about data thefts and losses when they occur. Victims are entitled to know how it happened, what was taken, whether the data was used, and so on. That should be standard procedure and ultimately, would be worth much more than the pittance that is usually offered today in these Dear John data letters -- free trials to credit monitoring services. Next time you receive a letter, look for the answers to Mike Cook's three questions. If you don't get them, complain to your congressional representative.