Hackers hit bank. Is your money safe anywhere?

October 3 2014, by Ken Sweet

In this Tuesday, July 16, 2013, file photo, an ATM is displayed at a Wells Fargo bank, in Atlanta. Hackers penetrated the computer systems of JPMorgan Chase & Co., the country's largest bank, stealing names, emails, addresses and phone numbers over the summer of 2014. The theft of personal information from 76 million households naturally raises questions about the safety of money in the digital era. (AP Photo/David Goldman, File)

Hackers stole personal information from millions of JPMorgan Chase customers this summer, in one of the biggest breaches of a financial company.

The bank says only non-financial data was taken—names, addresses, telephone numbers and email. But that's still a lot of personal detail, and experts warn that customers need to be vigilant about identity theft in the next several months.

The theft—involving 76 million households and seven million small businesses—raises questions about the safety of personal information, especially at banks. What risks do people face? Will this keep happening? And can bank customers reduce the threat of identity or financial theft?

Q: How concerned should I be if the hackers didn't get Social Security numbers, bank account or credit card information?

A: We may not yet know the full scope of what the hackers were able to steal, says Eric Chiu, president of HyTrust, a cloud security company based in Mountain View, Ca. "They can sit on your network for months, siphoning off data before being detected," says Chiu. He says that customers' addresses and phone numbers could be used or sold to others who might combine that information with other stolen data. It could then be used to access accounts or even to open new accounts in the unwitting customers' names.

Even if the information isn't used for phishing schemes or direct fraud, it could be sold on the gray market to people who might want to send spam or sales pitches to bank customers. "There's a good market for that kind of data," says Adam Kujawa, head of malware intelligence at Malwarebytes, a San Jose, California company that makes security software.

Q: How close did the hackers get to stealing customers' money or more sensitive financial data?

A: We don't really know. The hackers may not have been looking to siphon funds, says Chiu, because "data is what's gold now." Other security experts say the bank's public statements suggest that its defenses were partly successful, because hackers weren't able to get other information.

Q: So is this a partial win for the bank?

A: It might be, says Mike Lloyd, chief technology officer at Sunnyvale, Ca.-based RedSeal Networks. But the bank shouldn't declare victory—cybersecurity is "a never-ending war" against new and evolving threats.

Q: What else could happen?

A: One concern is that this breach was a reconnaissance mission in preparation for a bigger hack, says Craig Carpenter, chief strategist at AccessData, a cybersecurity firm. "They don't have to crack the entire system tomorrow," he says. "They could have simply been mining for data, or looking to leave something behind that would allow them to get into (JPMorgan's servers) easier next time."

Q: What else should banks do to protect customer data?

A: The financial industry is already doing more than other industries, says Dwayne Melancon, chief technology officer for the cybersecurity firm Tripwire, in Portland, Oregon. Chase in particular is known for using advanced security technology, says Avivah Litan, an analyst with Gartner, a technology research firm based in Stamford, Connecticut. But she also says that most companies have trouble keeping up with constant threats, and one big vulnerability lies with employees. While businesses tend to spend more on defending against outside attacks, many hacks begin with a compromised employee account. Litan says companies must do more to screen workers and also train them in security precautions.

Q: Should I close my account at JPMorgan?

A: At this point, there's no indication that's necessary. Steve Weisman, a Boston attorney and author of several books and articles about identity theft, says "it won't do any good" because other banks may be equally vulnerable to hacking. "There's no place to run and hide. You should monitor your account regularly and don't trust any communications you receive."

Q: After big attacks against retail chains and now Chase, should we expect more breaches?

A: The size and scope of the breaches are going to get worse, not better. Target, Home Depot and JPMorgan Chase are just the beginning, says Darren Hayes, a professor and expert in cybersecurity at Pace University in New York. It's safe to presume that hackers have been sitting inside these banks and business networks for months, even years, sometimes not doing anything. "Hackers these days are patient ... and are extremely effective at just gathering a lot of data over time."

Q: Is there any way to protect myself if they're this sophisticated?

A: Change your passwords regularly, don't click on links in suspicious emails (they could be phishing attempts by scammers), and regularly check online statements for any charges you don't recognize. Be wary of calls requesting personal information.

Q: How bad is the fallout so far?

A: The New York-based bank says there's no evidence of financial fraud associated with the breach.

Citation: Hackers hit bank. Is your money safe anywhere? (2014, October 3) retrieved 25 April 2024 from https://phys.org/news/2014-10-hackers-bank-money-safe.html