0-BankInfoSecurity-Chase Breach

Chase Breach Affects 76 Million Households

7 Million Small Businesses Also Impacted Jeffrey Roman (gen_sec) â€¢ October 2, 2014

See Also: Live Webinar | Making the Case for Managed Endpoint Detection and Response

JPMorgan Chase has confirmed that 76 million households and 7 million small businesses were impacted by a breach that reportedly began in June (see JPMorgan Chase Confirms Cyber-Attack).

“This breach is really serious - Chase is one of the most secure banks out there,” *[Worry]*says financial fraud expert Avivah Litan, an analyst at the consultancy Gartner. “It’s a national crisis. … We are all under attack, and this is not isolated to Chase.”

Sen. Edward J. Markey, D-Mass., who co-authored the Personal Data Protection and Breach Accountability Act, says: “The data breach at JPMorgan Chase is yet another example of how Americans’ most sensitive personal information is in danger. It is time to pass legislation to protect Americans against these massive data breaches.”

Details Revealed

The details of the number of households and small businesses affected by the June breach came to light Oct. 2, in a U.S. Securities and Exchange Commission Form 8-K submitted by JPMorgan Chase. The bank reveals that information compromised in the attack includes customers’ contact information, including names, addresses, phone numbers and e-mail addresses.

The breach affected customers who use these Web and mobile services: Chase.com, JPMorganOnline, Chase Mobile and JPMorgan Mobile.

But despite the theft of some account information, “there is no evidence that your account numbers, passwords, user IDs, date of birth or Social Security number were compromised during this attack,” the bank says. “We have not seen unusual fraud activity related to this incident.”

Internal Chase data - used in connection with providing or offering services to customers - also was compromised, the company says in a statement posted on its website.

JPMorgan Chase says it has cleaned up its systems following the attack and locked them down to prevent further attacks of this nature. “We have identified and closed the known access paths [of the attack],” the bank states in a FAQ posted to Chase.com. “We have no evidence that the attackers are still in our systems.” *[Rebuild]*

Chase has declined to offer free credit monitoring or identity theft protection services to customers whose data was stolen, since no financial or account information was compromised. As a result, “we don’t believe that you need to change your password or account information,” the company says.

Crisis of Confidence

Nevertheless, news of the breach will likely rock consumer confidence in the security of the financial system. *[Disappointment]* As Litan points out, “Chase is a completely different name than Home Depot or Target.”

“We expect banks to be safe,” *[Disappointment]*she adds. “They have so many regulations and invest so much in security and compliance. It’s a real slap in the face to know that they, too, can be attacked and breached. *[Disappointment]* I think everyone has to change their tactics. You have fight back. You have to go on the offense. You have to change your environment. And you have to make sure everyone on your staff is really aware and don’t ignore the signs when they suspect something is not right.”

Financial fraud analyst Al Pascual, an adviser for the consultancy Javelin Strategy & Research, says the breach at Chase proves the financial services

industry can be breached just as easily as retailers, *[Worry]* which have come under scrutiny for their poor security practices.

"While any breach is embarrassing, the fact that only less sensitive PII [personally identifiable information] was compromised was a lucky break," *[Positive]* Pascual says. "What I would be concerned about here is that the financial industry is trying to make the argument to regulators and other government officials that retailers are doing a poor job protecting consumer data and that they should be held to a higher standard. The Chase breach is so high-profile that it is undermining that effort."

No Second Cyber-Attack

Also on Oct. 2, the bank denied claims reported by The New York Times that a second attack had breached its network and systems *[Deny]*(see JPMorgan Chase: No New Cyber-Attack).

"The story is false," JPMorgan Chase spokeswoman Patricia Wexler tells Information Security Media Group. "We are not aware of any new breach."

The Times updated its story and revised its headline after Chase issued a statement refuting the newspaper's report. Initially, The Times reported that the nation's largest bank was, for the second time in three months, "scrambling to contain the fallout from a security breach of its vast computer network."

Breach Confirmed in September

News reports of an alleged breach at Chase first surfaced in late August. At that time, security experts said the breach was likely linked to a spear phishing attack that had compromised one of the bank's employees.

Chase confirmed the attack in mid-September. "We uncovered an attack by an outside adversary recently where the firm's technology environment was compromised," spokeswoman Kristin Lemkau told the The Times last month. "We are confident we have closed any known access points and prevented any future access in the same way." *[Rebuild]*

The breach allegedly began in June, but was not detected until late July, The Times reported in September.

Source of Breach

According to an Oct. 2 Wall Street Journal news report, hackers, believed to be based in Russia or Eastern Europe, likely breached the bank's network through the compromise of an employee's personal computer. From there, hackers reportedly penetrated other bank systems, an individual close to the investigation told The Journal.

"Employees often use software to tap into corporate networks from home through what are known as virtual private networks," the news report states. Chase reportedly has reset passwords used by every technology employee and disabled employee accounts that may have been compromised. *[Rebuild]*

Since discovering the intrusion, some 200 employees across J.P. Morgan's technology and cybersecurity teams have worked to examine data on more than 90 servers that were compromised, sources told The Journal. And a core team, led by Chase's chief operating officer, Matt Zames, oversaw the bank's breach-response strategy, the paper reports. *[Reinforce]*

Beware of Phishing

Going forward, Chase has warned its customers to be on the lookout for phishing attacks because the attackers gained access to their contact information. "We encourage you to be cautious of any communications that ask for your personal information," the bank says. "Don't click on links or download attachments in e-mails from unknown senders or other suspicious e-mail." *[Rebuild]*

Security experts support those social engineering warnings. *[Hope]* "The usual advice applies: If you get an e-mail or a call from a JPMorgan rep, feel free to thank them for contacting you and hang up," says Tod Beardsley, an engineering manager at security firm Rapid7. "Customers should always initiate that contact by looking at their credit card or

statement for the contact number; you simply can’t trust that an incoming call or e-mail is legitimate and not a phishing attempt.”

And John Zurawski, vice president of security firm Authentify, says small business customers of Chase impacted by the breach should take steps to ensure their employee and payroll accounts are secure. “Small businesses should immediately change their passwords,” he says. “The businesses affected should consent to any additional authentication factors the bank may offer.”

Tracy Kitten and Mathew J. Schwartz contributed to this story.