1-USA Today-JP Morgan

JP Morgan reveals data breach affected 76 million households

Elizabeth Weise

USATODAY

SAN FRANCISCO — The cyberattack on JPMorgan Chase & Co., first announced in July, compromised information from 76 million households and 7 million small businesses, the company revealed Thursday in a filing with the Securities and Exchange Commission.

Contact information, including name, address, phone number and e-mail address, as well as internal JPMorgan Chase information about the users, was compromised, the filing said. However the bank said no customer money appears to have been stolen.

JPMorgan said “there is no evidence that account information for such affected customers — account numbers, passwords, user IDs, dates of birth or Social Security numbers — was compromised during this attack.” *[Diminish]*

The attack is one of the largest corporate breaches thus far reported.

More chillingly, a report Thursday in The New York Times said that the hackers were able to gain “the highest level of administrative privilege” on more than 90 of the bank’s servers, according to people the newspaper spoke with who were familiar with the forensic investigation of the breach.

That means they “had root” on the servers of one of the largest banks in the world — they “could transfer funds, disclose information, close accounts, and basically do whatever they want to the data,” said Jeff Williams, chief technology officer with Contrast Security in Palo Alto, Calif.

In its SEC filing, JPMorgan said as of Oct. 2 it had not “seen any unusual customer fraud related to this incident.”

“This is a truly remarkable attack, but not just in its scope — hackers successfully penetrated one of the most secure organizations on this planet and they stole absolutely nothing of value — no money, no Social Security numbers, no passwords,” said John Gunn, with Vasco Data Security International in Chicago.

“Persistence like that, with no stolen money, is due to a future planned operation — or that the objective was to identify data that was material in some other aspect,” said J.J. Thompson of Rook Security in Indianapolis.

“This could be to track down a person of interest by observing financial transaction locations, to plans future large scale disruption when they know their competitor plans to wire funds to close a deal, or any other odd scenario you could see on (the TV show) ‘Blacklist,’” he said.

JPM shares were down 0.89% in after-hours trading. *[Anger]*

Whether there really was an attack or not, consumers should beware of “piggyback attacks” in which criminals launch social engineering attacks making use of customer anxiety after reports of a big-name breach.

“The usual advice applies: If you get an e-mail or a call from a JP Morgan rep, feel free to thank them for contacting you and hang up. 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,” said Tod Beardsley, engineering manager with security firm Rapid7.

About Us Newsroom Staff Ethical Principles Corrections Press Releases Accessibility Sitemap Terms of Service Your California Privacy Rights/Privacy Policy Privacy Policy

Do Not Sell My Info/Cookie Policy