PMorgan Chase Hack Affects 76 Million Households

By Jessica Silver-Greenberg, Matthew Goldstein and Nicole Perlroth
October 2, 2014 12:50 pmOctober 2, 2014 12:50 pm
Photo

The Manhattan headquarters of JPMorgan Chase, which securities filings revealed was attacked by hackers over the summer.Credit Andrew Burton/Getty Images

Updated, 9:03 p.m. | A cyberattack this summer on JPMorgan Chase compromised the accounts of 76 million households and seven million small businesses, a tally that dwarfs previous estimates by the bank and puts the intrusion among the largest ever.

The details of the breach — disclosed in a securities filing on Thursday — emerge at a time when consumer confidence in the digital operations of corporate America has already been shaken. Target, Home Depot and a number of other retailers have sustained major data breaches. Last year, the information of 40 million cardholders and 70 million others were compromised at Target, while an attack at Home Depot in September affected 56 million cards.

But unlike retailers, JPMorgan, as the largest bank in the nation, has financial information in its computer systems that goes beyond customers' credit card details and potentially includes more sensitive data.

“We’ve migrated so much of our economy to computer networks because they are faster and more efficient, but there are side effects,” said Dan Kaminsky, a researcher who works as chief scientist at White Ops, a security company.

Until just a few weeks ago, executives at JPMorgan said they believed that only one million accounts were affected, according to several people with knowledge of the attacks.

As the severity of the intrusion — which began in June but was not discovered until July — became more clear in recent days, bank executives scrambled for the second time in three months to contain the fallout and to reassure skittish customers that no money had been taken and that their financial information remained secure.

The hackers appeared to have obtained a list of the applications and programs that run on JPMorgan’s computers — a road map of sorts — which they could crosscheck with known vulnerabilities in each program and web application, in search of an entry point back into the bank’s systems, according to several people with knowledge of the results of the bank’s forensics investigation, all of whom spoke on the condition of anonymity.

Operating overseas, the hackers gained access to the names, addresses, phone numbers and emails of JPMorgan account holders. In its regulatory filing on Thursday, JPMorgan said that there was no evidence that account information, including passwords or Social Security numbers, had been taken. The bank also noted that there was no evidence of fraud involving the use of customer information.

Still, until the JPMorgan breach surfaced in July, banks were viewed as relatively safe from online assaults because of their investment in defenses and trained security staff. Most previous breaches at banks have involved stealing personal identification numbers for A.T.M. accounts, not burrowing deep into the internal workings of a bank’s computer systems.

Even if no customer financial information was taken, the apparent breadth and depth of the JPMorgan attack shows how vulnerable Wall Street institutions are to cybercrime. In 2011, hackers broke into the systems of the Nasdaq stock market, but did not penetrate the part of the system that handles trades.

Jamie Dimon, chief executive of JPMorgan Chase, says that the digital threat is on the rise.Credit Richard Drew/Associated Press Jamie Dimon, JPMorgan’s chairman and chief executive, has acknowledged the growing digital threat. In his annual letter to shareholders, Mr. Dimon said, “We’re making good progress on these and other efforts, but cyberattacks are growing every day in strength and velocity across the globe.”

Even though the bank has fortified its defenses against the attacks, Mr. Dimon wrote, the battle is “continual and likely never-ending.”

On Thursday, some lawmakers weighed in. Edward J. Markey, Democrat of Massachusetts and a member of the Senate Commerce Committee, said “the data breach at JPMorgan Chase is yet another example of how Americans’ most sensitive personal information is in danger.”

Hackers drilled deep into the bank's vast computer systems, reaching more than 90 servers, the people with knowledge of the investigation said. As they analyze the contours of the breach, investigators in law enforcement remain puzzled, partly because there is no evidence that the attackers looted any money from customer accounts.

That lack of any apparent profit motive has generated speculation among the law enforcement officials and security experts that the hackers, which some thought to be from Southern Europe, may have been sponsored by elements of the Russian government, the people with knowledge of the investigation said.

By the time the bank's security team discovered the breach in late July, hackers had already obtained the highest level of administrative privilege to dozens of the bank's computer servers, according to the people with knowledge of the investigation. It is still unclear how hackers managed to gain such deep access.

The people with knowledge of the investigation said it would take months for the bank to swap out its programs and applications and renegotiate licensing deals with its technology suppliers, possibly giving the hackers time to mine the bank's systems for unpatched, or undiscovered, vulnerabilities that would allow them re-entry into JPMorgan's systems.

Beyond its disclosures, JPMorgan did not comment on what its investigation had found. Kristin Lemkau, a JPMorgan spokeswoman, said that describing the bank's breach as among the largest was "comparing apples and oranges."

Preparing for the disclosure on Thursday, JPMorgan retained the law firm WilmerHale to help with its regulatory filing with the Securities and Exchange Commission, people with knowledge of the matter said. Earlier on Thursday, some executives — Barry Sommers, the chief executive of Chase's consumer bank — flew back to New York from Naples, Fla., where they had convened for a leadership conference, these people said.

The initial discovery of the hack sent chills down Wall Street and prompted an investigation by the Federal Bureau of Investigation. The bank was also forced to update its regulators, including the Federal Reserve, on the extent of the breach.

Faced with the rising threat of online crime, JPMorgan has said it plans to spend $250 million on digital security annually, but had been losing many of its security staff to other banks over the last year, with others expected to leave soon.