The New York Times

Hackers' Attack Cracked 10 Financial Firms in Major Assault

By Matthew Goldstein, Nicole Perlroth and David E. Sanger October 3, 2014 9:39 pm

Related Links

JPMorgan Chase Hack: Ways to Protect Yourself

Documents: JPMorgan's S.E.C. Filing

The huge cyberattack on JPMorgan Chase that touched more than 83 million households and businesses was one of the most serious computer intrusions into an American corporation. But it could have been much worse.

Questions over who the hackers are and the approach of their attack concern government and industry officials. Also troubling is that about nine other financial institutions — a number that has not been previously reported — were also infiltrated by the same group of overseas hackers, according to people briefed on the matter. The hackers are thought to be operating from Russia and appear to have at least loose connections with officials of the Russian government, the people briefed on the matter said.

It is unclear whether the other intrusions, at banks and brokerage firms, were as deep as the one that JPMorgan disclosed on Thursday. The identities of the other institutions could not be immediately learned.

The breadth of the attacks — and the lack of clarity about whether it was an effort to steal from accounts or to demonstrate that the hackers could penetrate even the best-protected American financial institutions — has left Washington intelligence officials and policy makers far more concerned than they have let on publicly. Some American officials speculate that the breach was intended to send a message to Wall Street and the United States about the vulnerability of the digital network of one of the world's most important banking institutions.

"It could be in retaliation for the sanctions" placed on Russia, one senior official briefed on the intelligence said. "But it could be mixed motives — to steal if they can, or to sell whatever information they could glean."

Ways to Protect Yourself After the JPMorgan Hacking
By TARA SIEGEL BERNARD

Consumers can lessen the risk of financial harm to themselves from big data breaches like the one at JPMorgan Chase.

The JPMorgan hackers burrowed into the digital network of the bank and went down a path that gave them access to information about the names, addresses, phone numbers and email addresses of account holders. They never made it into where the more critical financial information and personal information are stored.

The bank's security team, which first discovered the attack in late July, managed to block the hackers before they could compromise the most sensitive information about tens of millions of JPMorgan customers, said several security experts and others briefed on the matter. The attack was not completely halted until the middle of August and it was only in recent days that the bank began to tally its full extent.

American officials say they have been working with JPMorgan since the intrusion was detected, chiefly through the Treasury, the Secret Service and intelligence agencies that seek to find the source of the attacks. But that is slow work and one official cautioned against leaping to conclusions about the identities or the motives of the attackers.

"We've been wrong before," he said.

JPMorgan, the nation's largest bank, has begun contacting customers and making clear that no money was taken from any accounts. There has been no evidence of any fraudulent use of customer information. Most of the household accounts belong to United States residents. The hackers ended up with the addresses, email addresses and phone numbers of everyone who logged into JPMorgan's websites and mobile applications in the recent past.

Still, the recent attacks on the financial firms raise the possibility that the banks may not be up to the job of defending themselves. The attacks will also stoke

questions about regulations governing when companies must inform regulators and their customers about a breach.

"It was a huge surprise that they were able to compromise a huge bank like JPMorgan," said Al Pascual, a security analyst with Javelin Strategy and Research. "It scared the pants off many people."

Several financial regulators have warned that a coordinated attack on the banking system could set off another financial crisis.

On Friday, George Jepsen, the Connecticut attorney general, opened an investigation into the breach at JPMorgan, while Benjamin M. Lawsky, New York's top financial regulator, began calling bank officials to warn them to take the threat more seriously.

"There needs to be far more urgency," Mr. Lawsky said in an interview.

JPMorgan has also been working with law enforcement, including the F.B.I., since shortly after detecting the intrusion, which affected about 90 of the bank's computer servers. The bank said it believed that its systems were now secure and that the threat of the hackers' returning was over.

"To date, we have not seen any unusual fraud activity related to this incident," said Kristin Lemkau, a bank spokeswoman. "We have identified and closed the known access paths. We have no evidence that the attackers are still in our system. We have apologized to our customers."

But much remains unanswered about the intrusion, including just who the hackers are, which other financial institutions were hit and why the hackers went down a path inside JPMorgan's computer system that contained troves of customer information, but not financial data.

The intrusion also highlights a possible gap in United States regulations. Banks are not required to report data breaches and online intrusions unless the incident is deemed to have resulted in a financial loss to customers. Breach notification laws differ by state, but most laws require only that companies disclose a breach if

customer names were stolen in conjunction with other information like a credit card, Social Security number or driver's license number.

In some states, companies can wait up to a month to inform customers of a breach. Other state laws are more vague.

In California, for example, banks, companies and large organizations must inform the state attorney general's office and consumers about a breach without unreasonable delay — a rule that some companies interpret liberally, officials say. This year, Kamala Harris, the California attorney general, sued the Kaiser Foundation Health Plan, saying that it took four months for the foundation to disclose to some employees that their personal information may have been compromised.

For years, there have been attempts in Congress to force companies to inform customers more quickly when their information has been compromised, but recent bills have failed to muster enough support. One bill, sponsored by Senator Edward J. Markey, Democrat of Massachusetts, would create a clearinghouse where companies could exchange information about attacks.

United States bank executives say privately that they already share intelligence informally about attacks, which are occurring frequently on their systems.

This summer, Treasury Secretary Jacob J. Lew called on Congress to pass legislation that he said would bolster the information sharing process.

"As it stands, our laws do not do enough to foster information sharing and defend the public from digital threats," Mr. Lew said.

That the hackers were apparently able to move around JPMorgan's computer system undetected for several weeks is perhaps the most troubling aspect of the recent breach, officials at other large banks say.

The hackers were able to attain high administrative privileges within JPMorgan's network, rooting more than 90 servers and rummaging through customer databases with detailed information for 76 million households and seven million small-business online accounts.

As they looked around, according to one person with knowledge of the breach, the hackers gleaned some critical details of customers' accounts. With these, the hackers were able to determine whether the accounts fell within the private bank or in other business categories like mortgages.

Some people briefed on the results of the attack contend that it was only a matter of time before attackers could have gained access to customer funds and critical personal data.

Weeks into the attack, in mid-July, unusual behavior on the bank's network was spotted, and the attackers were stopped before they had a chance to pull any customer data back to their servers abroad.

But they did make off with one file which has unnerved executives. That file contained a list of every application and program deployed on standard JPMorgan computers that hackers can crosscheck with known, or new, vulnerabilities in each system in a search for a backdoor entry.

Swapping out those programs is costly and time-consuming, people say, because the bank would have to renegotiate licensing deals with technology suppliers and swap out programs and applications for hundreds of thousands of bank employees.

As one former employee explained: "It's as if they stole the schematics to the Capitol — they can't just switch out every single door and window pane overnight."

The attack came after a recent turnover within JPMorgan's information security group.

A number of staff members followed Frank Bisignano, JPMorgan's former co-chief operating officer, to First Data last year. This year, First Data agreed to pay JPMorgan over accusations that by wooing other executives to the payment processor, Mr. Bisignano had violated the terms of his former employment contract.

By then, First Data had already hired JPMorgan's chief information officer, Guy Chiarello; its cybersecurity czar, Anthony Belfiore; its head of compliance, Cindy Armine; and Tom Higgins, JPMorgan's head of operation control.

Anish Bhimani, the bank's chief information risk officer, remained. Mr. Bhimani, who is well respected in the cybersecurity industry, is a co-author of a 1996 book on cybersecurity, "Internet Security for Business."

Ms. Lemkau said the bank was pleased with its current cybersecurity personnel. "This is the highest-quality team we have ever had," she said.

Last December, JPMorgan hired Dana Deasy as chief information officer from BP. Greg Rattray, a former Air Force lieutenant colonel who specialized in cyberdefense was named the head of information security in June.

Challenges quickly followed. That same month, hackers found a way into the bank's systems.

Reporting was contributed by Michael Corkery, Nathaniel Popper, Peter Eavis and Jessica Silver-Greenberg.

A version of this article appears in print on 10/04/2014, on page A1 of the NewYork edition with the headline: Hackers' Attack Struck Systems at 10 Companies.