Wall Street Journal	New York Times
J.P. Morgan Says About 76 Million Households Affected By Cyber Breach **Bank, in Update on Previously Disclosed Data Breach, Says Hackers Got Contact Information But Not Logins**	**Cyberattack Against JPMorgan Chase Affects 76 Million Households**
J.P. Morgan Chase & Co. said about 76 million households were affected by a cybersecurity attack on the bank this summer in one of the most sweeping disclosed breaches of a financial institution. (¶1) The largest U.S. bank by assets said the unknown attackers stole customers' contact information—including names, email addresses, phone numbers and addresses. The breach, which was first disclosed in August and is still under investigation by the bank and law enforcement, extended to the bulk of the bank's customer base, affecting an amount equivalent to two-thirds of American households. It also affected about seven million of J.P. Morgan's small-business customers. It isn't clear how many of those households are U.S.-based. (¶2) The bank said hackers were unable to gather detailed information on accounts, such as account numbers, passwords, Social Security numbers or dates of birth. Customer money is "safe," the bank said in a statement to customers on Thursday. (¶3) J.P. Morgan reiterated that it hadn't seen unusual levels of fraud since the attack. It added that customers wouldn't be liable for any unauthorized transactions on the account if the bank is notified, and that customers don't need to change their passwords or account information. (¶4) With its wide scope of potential victims the latest incident is likely to renew concerns that hackers easily could wreak havoc with the nation's financial infrastructure. In 2011, the Journal reported that a hacking group possibly tied to Russia breached the computers of Nasdaq OMX, though there was no evidence anything was taken and trading systems weren't compromised. (¶5) While the incident is one of the broadest disclosed cyberattacks against a major financial institution, it likely isn't damaging to consumers, cybersecurity experts said. Several people familiar with the investigation and bank security said the data accessed appears to be related to J.P. Morgan's marketing functions rather than its banking operations. (¶6) If the J.P. Morgan hack was an old-fashioned bank heist, the hackers likely weren't steps away from the vault but "in the wrong building altogether," said James Lewis, a cybersecurity expert in Washington at the Center for Strategic and International Studies. (¶7) That makes it less concerning, said Drew Maness, an	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. (¶1) 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. (¶2) 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. (¶3) "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. (¶4) 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. (¶5) 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. (¶6) 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. (¶7) Operating overseas, the hackers gained access to the names, addresses, phone numbers and emails of JPMorgan account holders. In its regulatory filing on

independent cybersecurity consultant who used to work for Universal Music Group and Bank of America Corp. "But anytime someone walks in and takes information, it isn't good," he said. (¶8)

For instance, it is possible for hackers to use stolen email addresses to send fake emails to Chase customers that trick them into logging in to an impostor Chase website, Mr. Maness said. (¶9)

In August, hackers appeared to be targeting Chase customers with such emails, though it isn't clear if the incidents are related. (¶10)

In September, Home Depot Inc. confirmed its payment systems were breached in a cyberattack that impacted about 56 million payment cards. About a year ago, Adobe Systems Inc. said it suffered a cyberattack that some estimated impacted more than 100 million usernames, encrypted passwords and password hints. (¶11)

In addition, Target Corp.'s cyberattack last holiday season affected 40 million payment cards and 70 million names, addresses, emails and phone numbers. A few months later, the company's CEO resigned. (¶12)

At J.P. Morgan, the Federal Bureau of Investigation said in late August that it was working with the U.S. Secret Service to determine the scope of cyberattacks against American financial institutions. J.P. Morgan continues to work closely with law enforcement to determine the roots of the computer-hacking attack, people familiar with the matter said. (¶13)

The attacks focused on servers that housed user contact information of current and former customers who accessed chase.com or jpmorgan.com via the Internet or mobile devices in past years, these people said, though the time frame is unclear. The bank said it has 65 million Chase customers and four million small-business customers. (¶14)

Households can refer to individuals or an account housing multiple products like mortgage loans or separate checking accounts. Households and small businesses affected by the breach are within the bank's asset-management unit and community and consumer-banking unit, including customers who bank at Chase or use the bank's credit cards, they added. (¶15)

The attack at J.P. Morgan went unnoticed for about two months this summer, according to people familiar with the matter. Between mid-June and mid-August, hackers breached J.P. Morgan's servers for short intervals, around an hour at a time, these people said. J.P. Morgan learned of the attack in mid-August and stopped it, identifying and closing all access paths, these people said. (¶16)

The attack appears to have been caused by malicious

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. (¶9)

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. (¶10)

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. (¶11)

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." (¶12)

Even though the bank has fortified its defenses against the attacks, Mr. Dimon wrote, the battle is "continual and likely never-ending." (¶13)

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." (¶14)

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. (¶15)

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. (¶16)

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

computer code, known as malware, people familiar with the matter have said. Some people briefed on the investigation suspect a possible Russian or Eastern European link based on the style of the attacks and the bank target. (¶17)

Hackers appear to have originally breached J.P. Morgan's network via an employee's personal computer, a person close to the investigation has said. From there, the intruders were able to move further into the bank's systems. Employees often use software to tap into corporate networks from home through what are known as virtual private networks. (¶18)

The bank has reset passwords of every technology employee and disabled accounts that may have been compromised, people familiar with the bank's response said. Since mid-August, a couple hundred employees across J.P. Morgan's technology and cybersecurity teams have worked to examine data on over 90 servers that was compromised, these people said. (¶19)

A core team of around 20 J.P. Morgan employees oversaw the company's response to the cyberattack, led by its chief operating officer, Matt Zames. (¶20)

Mr. Zames sent a memo to employees Thursday evening detailing the scope of the attacks, adding that they are "highly unfortunate and are also a reminder that we all must be increasingly vigilant in the cyber world," according to a copy of the memo reviewed by The Wall Street Journal. (¶21)

Mr. Zames also reminded employees to make sure they have "fortified" their own defenses, such as logging off workstations, changing passwords often and choosing passwords that are hard for others to guess. He also reiterated that employees can't use work email for personal use, shouldn't open emails from anyone they don't know and should only use "reliable software." (¶22)

knowledge of the investigation. It is still unclear how hackers managed to gain such deep access. (¶17)

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. (¶18)

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." (¶19)

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. (¶20)

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. (¶21)

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. (¶22)

Correction: October 3, 2014
An earlier online only version of this article misstated where law enforcement officials and security experts believe the hackers were located. They are thought to be from Southern Europe, not Italy. (¶23)