David Lazarus

A simple theft nets Wells a world of woe
Break-in behind bar puts clients' data at risk

David Lazarus

Friday, November 21, 2003

A thief has stolen the names, addresses and Social Security numbers of thousands of Wells Fargo customers nationwide after breaking into the office of an East Bay business consultant and swiping his computers.

Wells Fargo is refusing to discuss details of the theft earlier this month or why the bank made such extensive information available to an outside contractor. Wells says the thief may not know that one of the stolen computers holds reams of proprietary data.

"We don't want to make the situation any worse than it is," said Doreen Woo Ho, president of Wells' consumer credit group, which handles the bank's home equity loans and personal lines of credit -- a $40 billion business with more than 2 million accounts.

The burglary illustrates that personal information doesn't have to be outsourced abroad to slip beyond a company's grasp. In this case, it traveled no farther than the desk of a financial analyst working out of a small office behind a Concord sports bar.

Woo Ho declined to specify how many of the group's customers nationwide were affected by the theft. "It's a very small percentage," she said, although she acknowledged that the number of accounts involved runs into the thousands.

The incident -- the first of its kind for Wells Fargo, according to Woo Ho -- came to light only this week when the bank mailed letters to affected customers informing them of the theft.

Richard Thompson, 55, a Benicia electrical technician and longtime Wells customer, received one of the letters. He said he was surprised by its lack of detail about the theft and its insistence that "Wells Fargo takes information security very seriously."

"Not seriously enough," Thompson grumbled. "As far as I'm concerned, this is as big a breach as they could have. It's like my money being stolen."

He also wonders why an outside consultant has Wells' customer information stored inside his office computer.

"It's outrageous," Thompson said. "My Social Security number is now out. This will affect me for the rest of my life."

Security has been a central question in the outsourcing of sensitive data to overseas contractors -- an increasing trend among U.S. companies. Last month, a woman in Pakistan doing clerical

work for UCSF Medical Center threatened to release patient files on the Internet unless the hospital helped her obtain money she felt she was owed.

The Wells Fargo case shows that data disasters can happen anywhere and that the most elaborate security precautions can be foiled by something as mundane as a purloined hard drive.

"We want you to know how deeply sorry we are that this has happened," the bank says in its letter to customers. "We apologize for any anxiety you may feel as a result ... We realize this news is troubling and sincerely apologize for any potential inconvenience or worry this may cause."

As for what did happen, the letter specifies only that "confidential information about your account was on one of the computers that was stolen."

Wells' privacy policy says customer information may be shared with third parties to help the bank conduct its business.

Lt. Gary Norvell of the Concord Police Department offered a more detailed account of the incident.

He said that before dawn on Saturday, Nov. 1, someone broke into offices behind Fatt's bar on Clayton Road. The entryway to the office suite apparently had been left unlocked. The doors on four offices within the suite were forced open.

Norvell said no losses were reported from three of the offices. "That was kind of strange," he observed.

One of the offices, however, reported the theft of a $1,000 painting, some CDs, a clock, a desktop computer and a laptop computer. The laptop, Norvell said, contained the information on Wells' customers.

Both he and Wells declined to identify the consultant whose computer was stolen.

It turns out, though, that the office belongs to a firm called EPS Consulting, run by Peter Gascoyne.

Gascoyne refused by telephone Thursday to discuss any aspect of the break- in or his relationship with Wells Fargo. He also wouldn't elaborate on the type of work he was doing for the bank or why personal information on thousands of Wells customers was stored in his laptop.

Wells Fargo's Woo Ho said only that Gascoyne is a "data analyst" and that he has a "special expertise" beyond what the bank was capable of doing in- house.

In 1997, Gascoyne wrote an article in a telecommunications-industry magazine in which he argued that businesses should use internal data to create statistical models for predicting future revenue.

"The impact of marketing campaigns and promotions can be more quickly and more accurately measured, which, in turn, can provide a competitive advantage and help improve the bottom line," he wrote.

Wells' letter to customers outlines a number of steps the bank is taking to try to mitigate the impact of the theft of the information.

It says the bank will monitor customers' credit accounts for unusual activity and reiterates a standing policy that "you will not be affected financially for any unauthorized activity on your Wells Fargo accounts."

Wells also says it will change all affected account numbers by the end of the month and will pay the $89.99 cost of a one-year membership in PrivacyGuard, a credit-monitoring service run by Trilegiant, a Connecticut marketing company.

Norvell at the Concord Police Department said local authorities were working with the Northern California Computer Crimes Task Force, a multi- jurisdictional team of cyber-sleuths, to track down the missing laptop. Investigators are looking into "a strong lead," he said.

Woo Ho apologized personally for the missing data. "We want customers to know how deeply we regret that this happened," she said.

Thompson, the Wells customer whose personal information was stolen with Gascoyne's computer, still can't believe that his privacy could be violated so easily.

"I think it's an outrage that our lives are no longer our own," he said. "I hope some attorney takes this and shoves it down the bank's throat."