HP Scandal Shines Light on a Simple, Treacherous Act

By Ellen Nakashima
Washington Post Staff Writer
Tuesday, September 19, 2006; D01

When Adam Yuzuk had a question about his cellphone bill, a Cingular Wireless agent told him to check his online account.

The only problem: He hadn't established one.

That day in June 2005, Yuzuk, a former president of a New York leather accessories firm, discovered someone had used his Social Security number and a fake e-mail address to set up his online account and view his calling records.

He learned this year, as part of a legal dispute with his former partners in the firm, that they had paid a private investigator to dig up information on him, including $300 for his phone records.

Yuzuk's case was featured at a congressional hearing in June, part of lawmakers' effort to curb pretexting -- the act of impersonating someone to obtain their personal records. The drive has gained fresh momentum with recent revelations that a firm hired by a Hewlett-Packard Co. subcontractor used the technique to obtain phone records of the firm's directors and journalists. A House subcommittee is probing HP's practices.

Federal legislation is pending that would criminalize the use of pretexting to obtain phone records. Some states have passed laws banning it, and states, phone companies and the Federal Trade Commission are suing data brokers who practice it. Despite such efforts, including a 1999 law banning pretexting to obtain financial records, the industry continues to thrive. It is driven by systemic weaknesses in retail, financial and other sectors; lax company security standards; and demand from lawyers, debt collectors, and even law enforcement and tabloid journalists, experts said.

"The simplicity of acquiring information like this is almost sad," said James Rapp, who made $1 million annually using the technique -- which included getting information on JonBenet Ramsey and Monica Lewinsky-- until he was convicted on racketeering charges and put out of business in 1999.

"Companies make a statement that we have privacy, but when it gets right down to it, if you or anybody calls up and asks for information on me, if you ask nice enough, they'll give it," Rapp said.

In June, Yuzuk, his voice trembling in anger, told a congressional panel his story: After he learned in June 2005 that his Cingular account had been hacked, he had a supervisor put a password on it and red-flag it -- moves that would keep his information safe from prying eyes, the supervisor assured him.
"I wanted the highest level of security possible," he told the House Energy and Commerce investigative subcommittee.

Then last April, Yuzuk legally obtained documents revealing that a former partner, Steve Kahn, had hired Michele Gambino of Gambino Information Services Inc. to retrieve his cellphone records.

Gambino Information Services, whose Web site notes the firm can conduct "informative telephone" conversations to "obtain various types of information," prepared a file for Kahn that included four months of phone bill detail, with two sets of records printed in September and October.

"This means that someone broke into my Cingular account two additional times after my account was password-protected and I was given what I believed was the highest level of security," he said.

In May, Cingular sued Gambino and Kahn in federal court in Atlanta. Kahn settled, but the case against Gambino continues, Cingular attorney David L. Balser said.

On Monday, Yuzuk and his former partners reached a settlement that includes a confidentiality clause forbidding them from discussing the case.

Reached for comment, Gambino said she was not interested in speaking to a reporter and hung up.

Rob Douglas, a former private investigator and now an information security consultant in Colorado, said Gambino has a degree of notoriety in the business.

It was Gambino who made the pretext call that gave a young New Hampshire man the work address of Amy Boyer, a former high school classmate he was obsessed with, according to the Boyer family's lawyer, David Gottesman. In October 1999, Liam Youens shot and killed Boyer at her workplace.

Then he killed himself.

Boyer's mother sued Gambino and the Internet investigative firm that had hired her for wrongful death and invasion of privacy. The case was settled.

"There has been no single event that has changed my life more than the murder of Amy," said Douglas, who was a consultant on the case and left the private investigation business in 2000. He said he is determined to stop the subterfuge. He called the fact that Gambino is still in business "unconscionable."

The business is a booming one, worth at least $30 million annually, congressional investigators estimate. When Rapp, 46, turned off the lights in his office for good, he had 15 employees and 1,500 clients. His employees went to work for others or started their own practices, he said.

"If you can make $200 an hour, literally, and you work a couple of hours a day, that's wonderful," he said. "You can make great money."

Firms that use pretexting, the number of which has multiplied through the ease of Internet advertising, offer quick results.

First Source Information, a Florida company, offered "1 to 2 hour turnaround time" with "volume discounts available," according to records obtained by the House committee. An online subsidiary, LocateCell.com,
which offered guarantees of "no data returned, no charge for the search," charged $110 for cellphone call records.

First Source was sued in December by Cingular and then by the state of Florida and other carriers. An Atlanta judge earlier this year ordered it to stop impersonating to obtain phone records, essentially shutting it down.

Douglas said firms that are closed often reappear under different names and that data brokers will repackage their services to get around laws. Despite the 1999 law criminalizing financial pretexting, he said, search firms are advertising services for obtaining financial records.

So how do they get the information? There are myriad ways, all playing off the company's willingness to please.

Setting up an online account is fairly easy once an investigator has a Social Security number, which can be obtained through commercial databases, Douglas said.

"You can go in and convince the phone company that the security code hasn't been set or needs to be reset, then you can go and change it to anything you want," Rapp said.

A more common way, he said, involves two calls.

In the first, an investigator poses as a customer to find out the balance, where to send the payment or how much was paid on the last bill.

With that data, Rapp said, "I call in a little bit later. I say I have an issue. I work for Acme Insurance and I get reimbursed for my expenses. I put out a little over two grand this month. I need that money, but I don't have everything I need."

Knowing the amount paid on the last bill establishes credibility. By saying that the call detail didn't appear on the bill, the investigator can cajole the operator into giving him an item-by-item recount, Rapp said.

E-mails and chat-room discussions on file with the House subcommittee's investigative panel shed more light on the practice.

Michele Yontef, an investigator whose skills have earned her the nickname "Ma Bell," asked a colleague in an August 2005 e-mail to help her get information on a Verizon cellphone number. "Merlindata (a commercial database) usually unblocks last 4 of SSN but on this target I cant get, do you have another database that possibly unblocks, if not, let me know and I will try to pretext it out of operator," she wrote.

Yontef, reached by phone last week, declined a request for an interview.

In a chat-room discussion in December, a participant identified as a Florida investigator wrote: "Many times the phone company will tell you that such and such is not available, but if you talk to the tech people, they'll tell you that they have it."

Authorities have focused their efforts on the data brokers but have largely ignored the brokers' clients. "There is mounting evidence that attorneys are top consumers of pretexting services," Chris Hoofnagle, former West Coast director of the Electronic Privacy Information Center, wrote in a February letter to state
bar ethics committees and the American Bar Association. The center has urged state ethics boards to review the technique under their ethical rules.

It also has identified dozens of Web sites that offer to obtain personal information through pretexting and has submitted the names of 40 such sites to the FTC for investigation and petitioned the Federal Communications Commission to protect individuals' phone records.

Larry Slade, a Los Angeles attorney for several data brokers, said his clients have long provided their services for free to law enforcement agencies. Until recently, that included obtaining phone records.

"I have a two-inch stack of documents, faxed requests from local, state and federal law enforcement," he said. "A lot of them are pre-investigative, whether they should pursue something, to help them identify possible suspects."

Paul Kilcoyne, an investigative director with the Department of Homeland Security's U.S. Immigration and Customs Enforcement, testified in June that agents in the Denver office "appeared to have used (data brokers) to quickly filter out numbers that were not related to their investigation. The data re-sellers were able to respond to these requests for information within a few days, whereas cellular phone companies typically take several weeks."

Kilcoyne's office is drafting guidelines that encourage agents in its field offices to discontinue use of such services. He noted that law enforcement officials have subpoena tools to obtain the data.

The House subcommittee will hold a hearing on HP on Sept. 28 and has called to testify outgoing HP chairman Patricia C. Dunn, general counsel Ann Baskins, global investigations manager Anthony Gentilucci, an outside counsel, a Boston security consultant and a Florida investigator.

The bottom line is, the phone companies need to tighten their security measures, said Jeannine Kenney, a senior policy analyst with Consumers Union.

"The carriers would very much like to act as though the only problem here are the bad actors fraudulently obtaining phone records," she said. But, "they share the records far too liberally with their contractors and other third parties. In some cases, they may sell it. They don't have sufficient safeguards in place to make sure someone can't fraudulently obtain it."

Staff researcher Richard Drezen and research editor Alice Crites contributed to this report.

© 2006 The Washington Post Company