



Database raid fallout escalates Confidential files on 400,000 may have been stolen; ChoicePoint, law enforcement differ on scope

More than 400,000 consumers may have been targeted for identity theft by a criminal ring that opened bogus business accounts with Alpharetta-based ChoicePoint — far more than previously reported.

Credit records nationally — not just the 35,000 or so in California as ChoicePoint said Tuesday — were accessed, the Los Angeles County Sheriff's Department said Wednesday.

"We know that there is a national number that is much larger than that," said Lt. Paul Denny of the sheriff's department. "We've used the number 400,000, but we're speculating at this point."

Executives at ChoicePoint, which maintains one of the largest databases of personal information in the country, acknowledged Wednesday that the number of potential victims is much larger than first thought. But they also suggested the actual number is lower than the law enforcement estimate.

The company said in a statement that "additional disclosures will be forthcoming to approximately 110,000 consumers outside of California whose information also may have been accessed."

James Lee, the company's marketing director, said ChoicePoint estimates that as many as 145,000 consumers are affected, including those in California. He said the company could not yet say what states other than California were affected, or whether any Georgia consumers were on the list.

Denny said investigators in California know of about 765 instances of financial charges being made to consumer accounts because the ring accessed ChoicePoint records.

The company had said Tuesday it knew of only one case, but acknowledged Wednesday the number of such instances is higher as well.

The criminals used stolen identities to establish accounts with ChoicePoint that gave them access to consumer data. They were able to pass through the screening process that ChoicePoint uses when businesses seek to access records.

ChoicePoint said it was "unable to discuss many specifics of the incident because law enforcement agencies have advised that release of any additional details could compromise the ongoing investigations."

The company's database of 10 billion business and personal records contains information from names and addresses to Social Security numbers and credit reports. With such information, criminals could steal identities and use the stolen identities to buy jewelry, consumer electronics and computers, Denny said.

One arrest has been made in the case. A 41-year-old Nigerian national, Olatunji Oluwatosin, was arrested Oct. 27 after he faxed an application for a ChoicePoint account from a Kinko's in Los Angeles.

That aroused suspicion at ChoicePoint, which notified sheriff's investigators. They sent a fax back, and Oluwatosin was arrested when he walked into the Kinko's to pick up the return fax.

The public was notified of the scam only last week, as ChoicePoint began notifying 35,000 Californians whose credit records were accessed.

California is the only state that requires that consumers be notified when their personal data has been disclosed illegally. Similar laws have been proposed elsewhere.

The incident has stirred privacy advocates calling for more regulation. In New York, a state legislator called on the state government to suspend contracts with ChoicePoint, MSNBC reported.

Denny said investigators believe Oluwatosin is not the only person involved in establishing the bogus accounts.

"What we know is that there were about 50 of these accounts," Denny said. At least three were used to access records outside the state, the sheriff's investigator said. He did not list the states.

ChoicePoint says it has strengthened its screening procedures as a result of the incident.

ChoicePoint clients — which include businesses, the government and law enforcement agencies — often use the database for pre-employment screening, in part to determine if people are who they say they are.

Asked if it was embarrassing that ChoicePoint's own screening system missed finding criminals using stolen identities, Lee said on Tuesday that it was "a little disconcerting."

Lee said finding the criminals is complicated because ChoicePoint could not in all cases track the data requests to the accounts making the request.