

Info Breach Puts Data Firm in Hot Seat

By **HARRY R. WEBER**

AP Business Writer

ATLANTA — Consumer data collector ChoicePoint Inc. says its mission is to arm customers with the information necessary to verify that the people they are doing business with are who they say they are.

That selling point has been turned on its head by bandits who were given access to the company's massive database by duping it into thinking they were someone they were not.

"The irony appears to be that ChoicePoint has not done its own due diligence in verifying the identities of those 'businesses' that apply to be customers," said Beth Givens, director of the Privacy Rights Clearinghouse, a nonprofit consumer advocacy group. "They're not doing the very thing they claim their service enables their customers to achieve."

Formed in 1997 as a spinoff of credit reporting agency Equifax, Alpharetta, Ga.-based ChoicePoint has rapidly grown beyond its roots of analyzing insurance claims information to become a clearinghouse for personal data on hundreds of millions of people.

The 19 billion public records in its database at its suburban Atlanta headquarters include everything from motor vehicle registrations, license and deed transfers, military records, names, addresses and Social Security numbers.

To a debt-collection firm, a company checking the background of a prospective employee, a journalist or a law enforcement agency, the one-stop shop ChoicePoint offers for obtaining personal information can be a lofty enterprise. To a criminal stealing identities, it's a gold mine.

The company acknowledged this week that thieves apparently used previously stolen identities to create what appeared to be legitimate businesses seeking ChoicePoint accounts. The bandits then opened up 50 accounts and received volumes of data on consumers, including names, addresses, Social Security numbers and credit reports.

The ring, which operated for more than a year before it was detected, used the information to defraud at least 750 people, according to investigators in California quoted by The Los Angeles Times. ChoicePoint estimates that as many as 145,000 people in California and other unnamed states may have been affected.

Like any business that opens an account with ChoicePoint, the suspect companies were given an access code and password that allowed them to use ChoicePoint's database. ChoicePoint says it puts applicants for accounts through rigorous protocols such as verifying business licenses and individual's names and background checks.

In this case, says ChoicePoint marketing director James Lee, the thieves — posing as check-cashing companies or debt-collection firms — provided business licenses that appeared to be legitimate and used the names of real people with clean criminal records.

The identities they used had not been reported stolen, so red flags were not initially raised, Lee said. The company caught on later to what was going on by tracking the pattern of the searches the suspects were doing, he said.

Lee said the company learned of the problem in October, but did not notify those customers who were possibly affected until this month because authorities did not want to jeopardize their investigation.

A man from North Hollywood, Calif., accused of stealing personal information from ChoicePoint pleaded no contest Thursday. Olatunji Oluwatosin, 41, was sentenced to 16 months in prison. Oluwatosin was arrested in October with five cell phones and three credit cards — all in other people's names, prosecutors said.

The incident is not the first time ChoicePoint has raised eyebrows.

A public outcry in April 2003 was created by an Associated Press report in which it was revealed that ChoicePoint bought official registry files listing sensitive data on tens of millions of people from sources in Costa Rica, Mexico, Colombia, Venezuela, Nicaragua, Guatemala, Honduras and El Salvador.

The government data, obtained through middlemen, was sold by ChoicePoint to law enforcement, immigration and other agencies. In the wake of the AP story, ChoicePoint said it had stopped gathering data in some countries, including Costa Rica and Mexico. The company also erased the Mexican data.

The sheer breadth of the information the company collects makes it any easy target for criminals, critics say.

In eight years, ChoicePoint has acquired roughly 60 companies, ranging from ones that provided insurance support to pre-employment background information to government support organizations. In so doing, it has grown from 20,000 clients to hundreds of thousands and now operates in 100 countries.

Privacy advocates say the data aggregation industry should be more regulated.

"It's not that these activities are inherently evil," said Daniel Solove, a privacy expert and law professor at George Washington University. "The problem is the individuals whose information is being used is out of the loop, often helpless and powerless to participate."

---