

500,000 at risk in ID theft scam

1,072 Delawareans will get a warning

By JOHN WAGGONER / USA Today

02/22/2005



ChoicePoint, a personal-information clearinghouse, is notifying almost 145,000 people nationwide - including more than 1,000 in Delaware - that their credit reports, Social Security numbers and other key personal data may have been stolen from the company's database.

California authorities say 500,000 people could be affected. "This is very, very big," says Jay Foley, co-executive director of the Identity Theft Resource Center.

ChoicePoint, based in Alpharetta, Ga., disputes the higher numbers. It is notifying affected people by mail and has purchased credit reports for them.

The thieves used stolen identities to open more than 50 bogus ChoicePoint accounts, posing as businesses seeking data. ChoicePoint discovered the fraud in October, closed the suspect accounts and informed law enforcement agencies.

The Delaware Attorney General's Office has yet to receive complaints from consumers related to the ChoicePoint security lapse, said Olha Rybakoff, director of the attorney general's consumer protection division. She said consumers concerned that they may have been victims of identity theft can call the attorney general's consumer hotline at (800) 220-5424.

If people receive notice from ChoicePoint that their information was compromised, they should put a fraud alert on their credit reports, Rybakoff said. Such an alert leads lenders to seek more verification of identity before extending credit and that could thwart a criminal, she said.

Rybakoff said the case highlights the significant threat posed by identity theft. She said a recent Federal Trade Commission report estimated that Delawareans lost \$2.5 million to identity theft in 2004.

"If information falls into the wrong hands, it can take years for the victim of the identity theft to get the problems cleared up," Rybakoff said.

ChoicePoint announced Jan. 15 that thieves had stolen data from as many as 35,000 Californians.

ChoicePoint said then that it had no evidence to indicate that the problem had spread to other states.

California authorities arrested Nigerian national Olatunji Oluwatosin, 41, in October during a sting operation in connection with the ChoicePoint case. Authorities say Oluwatosin had five cell phones and three credit cards in other peoples' names. He pleaded no contest Thursday and was sentenced to 16 months in jail. The California investigation is continuing.

Privacy advocates say the ChoicePoint breach is part of a larger problem.

"The story points out the inadequacy of regulation of companies that hold confidential information," said Edmund Mierzewski, identity theft expert with the U.S. Public Interest Research Group. "While consumers who seek a copy of their own credit report get the third degree, creditors and identity thieves alike are routinely given the key to the database vaults."

Consumers should sit tight until they hear from ChoicePoint, said Foley. "We don't want to start a mass hysteria."

Staff reporter Ted Griffith contributed to this article.

HOW TO ACTIVATE A FRAUD ALERT

Contact one of the major credit reporting companies:

- EQUIFAX: (800) 525-6285
- EXPERIAN: (888) 397-3742
- TRANSUNION: (800) 680-7289

You'll be opted out of all preapproved credit card and insurance offers for two years. The credit bureau will process your request for a free credit report within three business days.



More than 800 Iowans Victims of Credit Theft

Des Moines, February 22nd, 2005 - More than 800 Iowans are finding out they are victims of identity theft. Their social security numbers are among more than 140 thousand stolen last week by computer hackers.

The credit reporting agency Choicepoint says thieves used fake ID's to get into its computer system and steal financial information from people all over the country. Letters are going out to all the victims. Already, 750 victims reported the illegal use of their social security numbers.

Choicepoint says it will pay for one year of credit monitoring for everyone who had their information stolen.