

ChoicePoint Fraud Case Shows Need for Security Controls

Avivah Litan

A ChoicePoint security breach demonstrates another technique criminals can use to steal consumer information. Enterprises must tighten access to data, and government must better protect consumers and punish lax security.

NEWS ANALYSIS

Event

On 16 February 2005, ChoicePoint, a company that sells personal data to governments and businesses, reported that thieves had gained unauthorized access to its data on 145,000 consumers in the United States. The data include names, addresses, Social Security numbers and credit reports. ChoicePoint said the thieves set up fake companies to get access to the data. The incident happened in October 2004, but ChoicePoint did not disclose it until later, and then initially only to consumers in California, which has a state law that requires such disclosure.

Analysis

Fraudulent access to credit reports is a persistent problem. Some companies that have legitimate access to credit reports do not effectively control access to credit reports within the company. Bogus companies, such as fake mortgage brokers, are frequently set up to look legitimate, for the purpose of stealing consumers' financial information.

Consumers who may have been hurt cannot protect themselves from future identity theft. They can put an alert on their credit files, to find out whether their information has been stolen. This will not, however, tell them whether thieves are just using their Social Security numbers with other names or criminals have acquired forged driver's licenses and passports with their information.

This case hurts ChoicePoint's reputation, but it also harms credit bureaus and other data sources that passed their reports through ChoicePoint. This incident shows how enterprises must take a multipronged approach to fraud prevention. Strong authentication does nothing if you are authenticating a bogus transaction. Data encryption does nothing if crooks pose as legitimate entities to gain open access to the data.

Recommendations for enterprises:

- Tighten access controls on credit reports and other sensitive data.
- Subscribe to better fraud protection systems, so that when these stolen identities begin to be used, they are detected through behavior pattern recognition.
- If you are a victim of fraud, notify consumers immediately and fully.

Recommendations for government:

- Make bureaus and third parties legally responsible for fraud if they do not follow certain security and due diligence measures.
- Update laws so that disseminators of data from credit bureaus and other sensitive sources do more due diligence concerning who gets access to their data.
- Expand the California disclosure law nationwide, and require enterprises to notify consumers promptly if their data is accessed without authorization.

Analytical Source: Avivah Litan, Gartner Research

Recommended Reading and Related Research

- "U.S. Banks Should Heed Regulator's Security Advice" — The Federal Deposit Insurance Corp. report on bank security has important advice for banks that want to protect against unauthorized access to customers' accounts. **By Avivah Litan**
- "U.S. Consumer Fraud Spreads Its Tentacles Across Channels" — Criminals use multiple methods and channels to steal consumer information, identities and money, but online fraud is increasing the fastest. **By Avivah Litan and John Pescatore**

(You may need to sign in or be a Gartner client to access the documents referenced in this FirstTake.)

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Level 7, 40 Miller Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Latin America Headquarters
Av. das Nações Unidas 12.551
9 andar—WTC
04578-903 São Paulo SP
BRAZIL
+55 11 3443 1509