

ChoicePoint to Pay Fine for Second Data Breach

Grant Gross, IDG News Service

Oct 19, 2009 12:40 pm – [Direct Link](#)

Data broker ChoicePoint, the victim of a 2004 data breach affecting more than 160,000 U.S. residents, has agreed to strengthen its data security efforts and pay a fine for a second breach in 2008, the U.S. Federal Trade Commission said Monday.

ChoicePoint, now a subsidiary of Reed Elsevier, will pay US\$275,000 to resolve the newest [FTC complaint](#). The FTC accused the company of failing to implement a comprehensive information security program to protect consumers' personal information, as required by the agency after the 2004 breach.

The April 2008 breach compromised the personal data of 13,750 people, the FTC said in a press release. ChoicePoint turned off a "key" electronic security tool used to monitor access to one of its databases, and failed to detect that the security tool was turned off for four months, the FTC said.

For a 30-day period, an unknown hacker conducted thousands of unauthorized searches of a ChoicePoint database containing sensitive consumer information, including Social Security numbers, the FTC said. After discovering the breach, the company notified the FTC.

If the software tool had been working, ChoicePoint likely would have detected the intrusions "much earlier," the FTC said.

A ChoicePoint representative wasn't immediately available for comment on the new court order.

Under a modified court order, ChoicePoint is required to report to the FTC detailed information about how it is protecting the breached database and certain other databases and records containing personal information. The ChoicePoint reports are required every two months for two years.

The 2004 data breach, reported by ChoicePoint in 2005, resulted in at least 800 cases of identity theft, the FTC said. A settlement and 2006 court order required the company to \$15 million in civil penalties and consumer redress.

In the earlier settlement, ChoicePoint agreed to maintain procedures to ensure that sensitive consumer reports were provided only to legitimate businesses for lawful purposes; to maintain a comprehensive data security program; and to obtain independent assessments of its data security program every other year until 2026.