LexisNexis admits to another major data breach

by Angela Moscaritolo

May 04, 2009

About 32,000 people are being notified that their personal information may have been compromised after a breach at consumer data provider LexisNexis resulted in identity theft and credit fraud, the company has disclosed.

According to the breach notification letter LexisNexis began sending on Friday, the thieves operated businesses that were former customers of data aggregator and credentialing service ChoicePoint, which was acquired last year by LexisNexis parent Reed Elsevier.

Using personal information of U.S. residents obtained from LexisNexis and fraudulent mail boxes in the United States, criminals applied for and obtained bogus credit cards. The scheme is linked to a Nigerian scam artist, according to CBS News, which first reported the breach.

The U.S. Postal Inspection Service (USPIS), in a statement issued Monday, said it was investigating the data breach. It would not reveal details, but said a total of 40,000 notification letters were being sent, and 300 actual identity theft victims already have been notified.

Criminals may have had access to individuals' personal information, including names, birth dates, and Social Security numbers between June 14, 2004 and Oct. 10, 2007, according to LexisNexis. So not to compromise the integrity of the investigation, LexisNexis was instructed by USPIS to delay notifying individuals whose information was compromised.

Further details of the breach have not been disclosed because the federal investigation is still ongoing, USPIS spokesman Peter Rendina told SCMagazineUS.com Monday.

Investigative Professionals, a Santa Fe, N.M.- based company that performs background checks, also is involved in the breach, according to the CBS report. When contacted by SCMagazineUS.com Monday, an executive for the company said he was instructed by postal investigators not to comment about the breach due to the ongoing probe.

In 2005, ChoicePoint experienced a breach in which criminals, posing as customers, stole the personal information of 163,000 people. The incident served as a watershed moment in terms of disclosure to victims and creation of state laws around breach notification. ChoicePoint ultimately was ordered to pay $15 million in fines and customer redress.

The same year, LexisNexis suffered a breach in which intruders may have accessed personal data of up to 310,000 Americans.

Eduard Goodman, general counsel and chief privacy officer for vendor Identity Theft 911, told SCMagazineUS.com Monday that for companies such as ChoicePoint that maintain huge repositories of consumer information they sell to law enforcement and other organizations, breaches are a cost of doing business. No matter how well companies vet the businesses they sell to, there always will be fraudsters trying to get their hands on the information, he said.

“It doesn't surprise me,” Goodman said. “That's the problem with companies whose entire business is buying and selling information.”

LexisNexis said in the notification letter that it has beefed up its security and privacy safeguards over the past several years. This includes implementing a standards-based security control framework; limiting access to sensitive personally identifiable information and requiring potential customers to undergo a multistep verification process to ensure their business is legitimate.

The company is offering affected individuals one year free credit monitoring.

Topics:

- Retail
- Cybercrime
- Data Breach
- Data Breach

- Cyberthreats

Related Links

- LexisNexis