LexisNexis says it had data breach earlier this year

September 26 2013, by Christopher Seward

LexisNexis, one of the country's largest collectors of personal information on individuals and businesses, said it is trying to determine whether hackers may have gained access to Social Security numbers, background reports and other details on millions of Americans during a data breach earlier this year.

The global company, which has one of its operations based in Alpharetta, Ga., acknowledged to The Atlanta Journal-Constitution that there was a breach, but said that so far there is "no evidence that customer or consumer data were reached or retrieved" by hackers. The breach appears to date back at least as far as April and was first reported by KrebsOnSecurity, a computer security blog by former Washington Post reporter Brian Krebs.

LexisNexis' wide-ranging databases, which are built from public records and proprietary sources, are used for identity checks, employee screenings, debt collections and more. Its clients include government agencies, insurers, banks, media companies, corporate personnel offices and private investigators. In addition to Alpharetta, the company has operations in Atlanta and Duluth, Ga.

LexisNexis became a global powerhouse in information gathering when its parent, London-based publishing company Reed Elsevier, purchased Alpharetta-based ChoicePoint, a reseller of credit data, for $4.1 billion in 2008.

Data breaches have become commonplace, with daily reports of institutions from banks to health care providers falling victim to hackers. Paul Stephens, director of policy and advocacy at the Privacy Rights Clearinghouse, said that while victims of data breaches don't necessarily become victims of identity thefts, "unfortunately, data breaches are extremely common, and they can in many instances lead to identity thefts." According to Javelin Strategy & Research, more than 12.6 million adults were victims of identity theft in the U.S. last year, and identity theft is the No. 1 complaint filed with the Federal Trade Commission.

LexisNexis spokesman Stephen Brown said the company would not discuss whether it has informed consumers and its clients about the breach.

This is isn't the first time LexisNexis has dealt with a breach. In 2005, the personal data on as many as 310,000 consumers was exposed, including Social Security numbers and driver's license information. Before it was acquired by Reed Elsevier, ChoicePoint was fined $10 million in 2006 over a failure to protect the personal data of 145,000 people who fell victim to identity thieves a year earlier.

Brown told the Journal-Constitution the company is working with the FBI and outside forensic investigators to determine the extent of any breach.

"In that investigation, we have identified an intrusion targeting our data but to date have found no evidence that customer or consumer data were reached or retrieved," spokesman Stephen Brown said. "Because this matter is actively being investigated by law enforcement, I can't provide further information at this time."

Lindsay Godwin, an FBI spokeswoman in Washington, confirmed an

investigation was underway and that it involved several companies.

In his blog, Krebs said he conducted a seven-month investigation that revealed two LexisNexis servers were hacked by what he called an online identity theft operation. Neither LexisNexis nor the FBI would provide information on the operation.

People seeking Social Security or other personal data from the operation pay as little as 50 cents per record, according to Krebs.

In addition to LexisNexis, Krebs said hackers also may have gained access to similar data provided by two other companies, Dun & Bradstreet and Kroll Background America Inc., a unit of Altegrity.

Krebs said hackers installed unauthorized software on the companies' servers. The hackers remotely controlled a collection of computers, or a botnet, as far back as April 10 in the case of LexisNexis, Krebs said.

Krebs said LexisNexis confirmed two of its servers were compromised. Short Hills, N.J.-based Dun & Bradstreet's systems were compromised at least as far back as March 27, Krebs said. A server at Kroll Background America Inc., which provides employment background checks and drug screenings, also was compromised. A Dun & Bradstreet spokesman told Krebs the company is "aggressively investigating the matter," but Altegrity would not confirm nor deny a breach had occurred.

Stephens, of the Privacy Rights Clearinghouse, said the steps individuals should take to protect themselves from identity theft depend on the data stolen.

Consumers should consider placing a 90-day fraud alert on their credit report if it shows unfamiliar activity or a security freeze in more serious cases, such a stolen Social Security number.

Stephens added that identity theft may not show up for months after a data breach has occurred.

©2013 The Atlanta Journal-Constitution (Atlanta, Ga.)
Distributed by MCT Information Services

Citation: LexisNexis says it had data breach earlier this year (2013, September 26) retrieved 20 September 2024 from https://phys.org/news/2013-09-lexisnexis-breach-earlier-year.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.