

LexisNexis breach reveals 'secret questions'

CYBERTRUTH (/BLOG/CYBERTRUTH/)

Byron Acohido, USA TODAY

4:56 p.m. EDT September 27, 2013



(Photo: USA TODAY)

SHARE

59

CONNECT

56

TWEET

<https://twitter.com/intent/tweet?url=http://usat.ly/19Gjlco&text=LexisNexis%20breach%20reveals%20secret%20questions>

SEATTLE – The systematic theft of records from three major U.S. data aggregation companies could well turn out to be much more damaging to consumers than any previous large-scale theft of credit card data.

"This is a much bigger deal than a regular credit card database breach," says Avivah Litan, banking security analyst at Gartner.

Cybersecurity blogger Brian Krebs conducted a [seven-month investigation](http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/)

[\(http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/\)](http://krebsonsecurity.com/2013/09/data-broker-giants-hacked-by-id-theft-service/) to document how a crime group, known as the SNSDOB gang, has systematically stolen personal data from LexisNexis, Kroll Background America and Dun & Bradstreet --and then channeled that data to hard-core identity thieves.

CONTEXT: [How data aggregators loosely handle personal data. \(http://lastwatchdog.com/credit-bureaus-created-perpetuate-errors-credit-history/\)](http://lastwatchdog.com/credit-bureaus-created-perpetuate-errors-credit-history/)

All of this is possible because the data brokers tap public sources to gather up details of how we live our lives. The financial and insurance industries then tap this information to support a system referred to as Knowledge Based Authentication, or KBA, also referred to as "shared secrets." These are so-called "out of wallet" questions that only you, presumably, should know the answers to.

Typical KBA queries might ask you to name your primary mortgage holder, or say where you lived 10 years ago, or name where you met your spouse.

Sourced by the data brokers, KBA enables you to use the phone or the Internet to take out a mortgage, withdraw cash from your 401K, apply for health coverage and conduct other transactions. KBA helps financial and insurance companies to cut costs and expand profit-making services.

But KBA has turned out to be a boon for cybercriminals and identity scammers.

Criminals are able to readily purchase KBA data in the cyberunderground. This empowers them to impersonate victims to take out mortgages, extract funds from pension funds and apply for health coverages.

Consumers have tolerated round after round of huge data breaches in which their credit and debit card numbers are stolen and land in the hand of criminals. That's because the payments industry generally makes them whole, in cases where a stolen payment card number is used for theft or fraud.

But once you get beyond fraudulent credit card use, consumer protections are scarce.

"If someone takes out a loan in your name because they're able to answer KBA questions you have no protection, it could take years to recover and it's a huge hassle," says Litan. "Let's say it's your pension. Your 401K could be drained, and there's no legal protection. Your financial institution is not required by law to make you whole. And one way the bad guys are able to take your money out is by answering these secret questions."

SHARE

59

CONNECT

56

TWEET

<https://twitter.com/intent/tweet?url=http://usat.ly/19Gjlco&text=LexisNexis%20breach%20reveals%20secret%20questions>