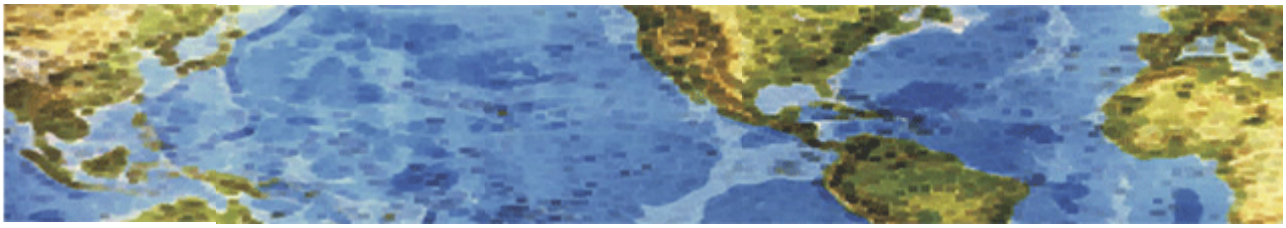
HALL ASSOCIATES



Risk-Based Decision Making Commentary
5 April 2014 Newsletter

U.S. States Investigating Breach at Experian

This is a story on how the existing cybercrime underground could get our personal and financial information. Identity theft is pervasive and everyone should minimize where your information is and to lock down your information as much as possible..

An exclusive KrebsOnSecurity investigation detailing how a unit of credit bureau Experian ended up selling consumer records to an identity theft service in the cybercrime underground has prompted a multi-state investigation by several attorneys general, according to wire reports. Reuters had a story this afternoon quoting Illinois Attorney General Lisa Madigan saying that "it's part of a multistate investigation," and that Connecticut Attorney General George Jepsen said that Connecticut is looking into the matter as well.

News of the breach first came to light on this blog in October 2013, when KrebsOnSecurity published an exclusive story detailing how a Vietnamese man running an online identity theft service bought personal and financial records on Americans directly from a company owned by Experian, one of the three major U.S. credit bureaus. Hieu Minh Ngo, a 24-year-old Vietnamese national, pleaded guilty last month to running an identity theft service out of his home in Vietnam. Ngo was arrested last year in Guam by U.S. Secret Service agents after he was lured into visiting the U.S. territory to consummate a business deal with a man he believed could deliver huge volumes of consumers' personal and financial data for resale.

But according to prosecutors, Ngo had already struck deals with one of the world's biggest data brokers: Experian. Court records just released last week show that Ngo tricked an Experian subsidiary into giving him direct access to personal and financial data on more than 200 million Americans.

According to U.S. government investigators, the data was not obtained directly from Experian, but rather via Columbus, Ohio-based US Info Search. US Info Search had a contractual agreement with a California company named Court Ventures, whereby customers of Court Ventures had access to the US Info Search data as well as Court Ventures' data, and vice versa. Experian came into the picture in March 2012, when it purchased Court Ventures (along with all of its customers — including Mr. Ngo). For almost ten months after Experian completed that acquisition, Ngo continued siphoning consumer data and making his wire transfers.

A transcript of Ngo's guilty plea proceedings obtained by KrebsOnSecurity shows that his ID theft business attracted more than 1,300 customers who paid at least $1.9 million between 2007 and Feb. 2013 to look up Social Security numbers, dates of birth, addresses, previous addresses, phone numbers, email addresses and other sensitive data on more than three million Americans.

http://krebsonsecurity.com/2014/04/u-s-states-investigating-breach-at-experian/

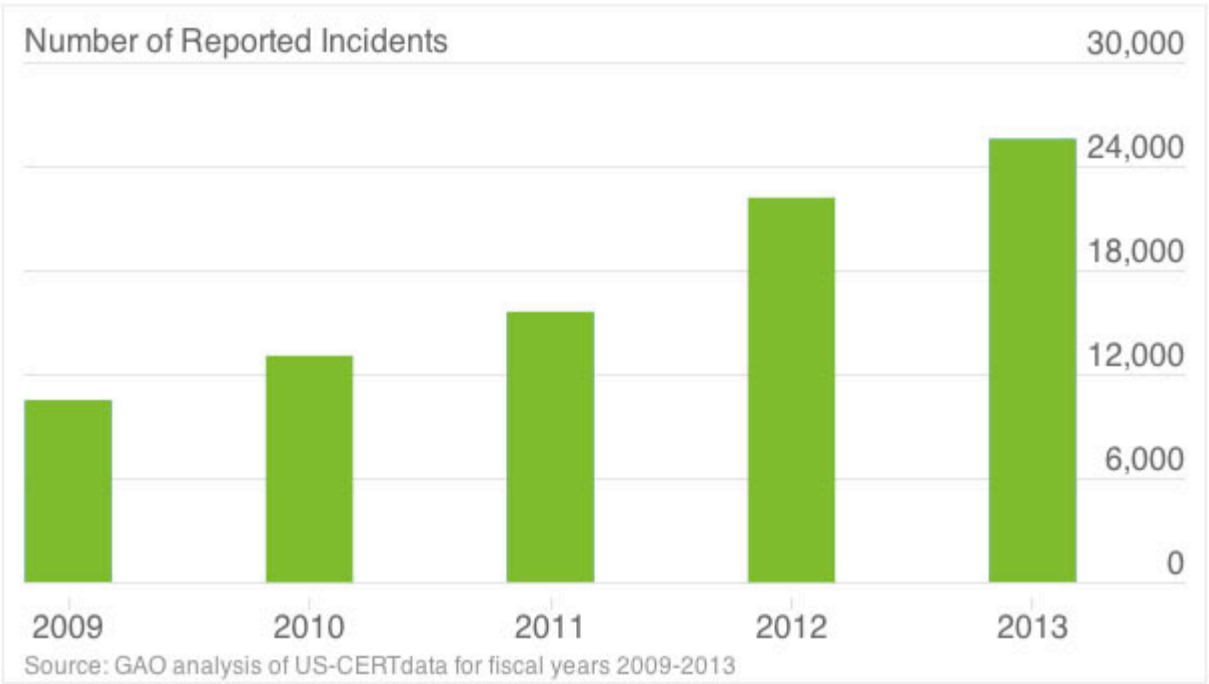
HALL ASSOCIATES

One Chart Shows Why You Shouldn't Trust the Feds With Your Data

There has been a spike in government data breaches that has compromised the personal information of federal employees and citizens. A report released Wednesday by the Government Accountability Office shows that security incidents involving personally identifiable information more than doubled between 2009, when there were 10,481 such breaches, and 2013, when the number climbed to 25,566.

Collectively, the breaches affect hundreds of thousands of people and cost taxpayers millions of dollars. For example, in July 2013, hackers stole a variety of information, including Social Security numbers, bank account numbers and security questions and answers associated with more than 104,000 individuals from an Energy Department computer system. According to Energy's inspector general, the costs of assisting affected individuals and lost productivity stemming from the breach could top $3.7 million, GAO noted.

Among other problems, GAO noted that only one of seven agencies reviewed by auditors correlated an assigned risk level with breaches of personal information and none of the seven consistently documented lessons learned from their breach responses.



http://www.nextgov.com/cybersecurity/cybersecurity-report/2014/04/one-chart-shows-why-you-shouldnt-trust-feds-your-data/81844/?oref=nextgov_today_nl