Experian Lapse Allowed ID Theft Service Access to 200 Million Consumer Records — Krebs on Security

In October 2013, 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. Today's story looks deeper at the damage wrought in this colossal misstep by one of the nation's largest data brokers.

Vietnamese national Hieu Minh Ngo pleaded guilty last week to running the ID theft service Superget.info.

Last week, **Hieu Minh Ngo**, a 24-year-old Vietnamese national, pleaded guilty 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.*

HIEU KNOWS YOUR SECRETS?

As I reported last year, 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.

Posing as a private investigator operating out of Singapore, Ngo contracted with Court Ventures, paying for his access to consumer records via regular cash wire transfers from a bank in Singapore. Through that contract, Ngo was able to make available to his clients access to the US Info Search database containing Social Security, date of birth and other records on more than 200 million Americans.

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.

Ngo's ID theft business attracted more than 1,300 customers who paid at least $1.9 million between 2007 and Feb. 2013

Until last week, the government had shared few details about the scope and the size of the data breach, such as how many Americans may have been targeted by thieves using Ngo's identity theft service. According to a transcript of Ngo's guilty plea proceedings obtained by KrebsOnSecurity, Ngo's 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.

The government alleges that the service's customers used the information for a variety of fraud schemes, including filing fraudulent tax returns on Americans, and opening new lines of credit and racking up huge bills in the names of unsuspecting victims. The transcript shows government investigators found that *over an 18-month period ending Feb. 2013, Ngo's customers made approximately 3.1 million queries on Americans.*

"At this point the government does not know how many U.S. citizens' [personally identifiable information] was compromised, although that information will be available in the near future," **U.S. Attorney Arnold H. Huftalen** told **Judge Paul J. Barbadoro** in New Hampshire District Court earlier this month. "And we don't know because the way the process worked was a bad actor could type in the name of an individual and a state..."

Huftalen's explanation was interrupted by Judge Barbadoro, who told the courtroom he was late for another engagement.

However, based on my own experience with Ngo's service, I believe Mr. Huftalen was trying to explain that because of the way that Ngo set up his identity theft service — variously named "Superget.info" and "findget.me" — each customer query in fact returned multiple records.

The "sourceid" abbreviations in Ngo's Superget.info identity theft service pointed toward Court Ventures.

When I first became aware of Superget.info, I conducted a search on my own information, asking Ngo's service to return any information on a Brian Krebs in Virginia. That query produced several pages of results, with each page containing at least ten different records full of personal data on multiple individuals — including my correct records. Revealing the more sensitive data for each record — including the date of birth and Social Security number — merely required clicking a link within each listing on the page; each click would result in a small amount being deducted from the customer's balance.

The point is that each query on Ngo's service almost always exposed multiple records. That means that if Ngo's clients conducted 3.1 million individual queries, the sheer number of records exposed by Ngo's service is likely to have been many times that number — *potentially as many as 30 million records.*

EXPERIAN: 'WE'RE GOING TO MAKE SURE THEY'RE PROTECTED'

Beyond acknowledging the broad outlines of the government's claims against Ngo, Experian has refused to discuss the matter. "Due to an ongoing federal investigation, we have been asked not to comment beyond the information we have already shared to ensure nothing impedes the progress of the investigation," Experian spokeswoman **Susan Henson** said in an emailed statement.

Experian's Tony Hadley, addressing the Senate Commerce Committee in Dec. 2013.

The few public statements that Experian has made regarding the incident came in a hearing last December before the Senate Committee on Commerce, Science, & Transportation, which was examining the data broker industry.

In that hearing, **Missouri Senator Claire McCaskill** grilled **Tony Hadley**, Experian's senior vice president of government affairs. Every other senator on the committee focused on Experian's practice of profiling consumers, but McCaskill used her time to question Hadley specifically about the company's role in Ngo's ID theft service.

Hadley acknowledged that Experian failed to conduct the due diligence needed to detect Ngo's activities prior to or anytime after acquiring Court Ventures. Indeed, Hadley said that Experian didn't learn about Ngo's activities until after being notified by the U.S. Secret Service.

"During the due diligence process, we didn't have total access to all the information we needed in order to completely vet that, and by the time we learned of the malfeasance nine months had expired, and the Secret Service came to us and told us of the incident," Hadley told McCaskill and other panel members. "We were a victim, and scammed by this person."

The Missouri Democratic senator shot back: "Well I would say people who had all their identities stolen are the real victims."

"And we know who they are, and we're going to make sure they're protected," Hadley assured the panel. But incredibly, in the very next breath Hadley seemed to suggest that nobody had proven or alleged that any of the records its company sold to Ngo

had resulted in harm to consumers.

“There’s been no allegation that any harm has come, thankfully, in this scam,” Hadley said.

I asked Experian to explain the apparent inconsistencies in Mr. Hadley’s statement, and to clarify whether the company had already begun to offer protection or service to anyone impacted by this scheme. So far, the company has declined to respond to those questions, citing the ongoing investigation.

But the evidence offered by the U.S. government strongly suggests that many people were injured by Experian’s lack of due diligence. Addressing the court at Ngo’s guilty plea hearing last week, U.S. Attorney Arnold H. Huftalen said the evidence was clear that Ngo’s customers purchased data from Experian’s firm with the intention of stealing the identities of consumers.

“The U.S. Secret Service has conducted investigations into many of his customers, all of whom have stated that they only obtained the information from Mr. Ngo to engage in criminal fraud,” Huftalen said. “The evidence would establish that at the time Mr. Ngo knew that he was providing the information for others to engage in fraud.”

It remains unclear whether Experian will ever be required to answer for its costly oversight. Mr. Ngo, on the other hand, is facing a lengthy prison sentence. He is charged with wire fraud, access device fraud and identity fraud. The maximum possible prison term for all three offenses combined is 45 years. Ngo may also be fined up to twice the gross gain resulting from his offenses, or twice the loss to consumers, whichever is greater. Ngo is slated to be sentenced on June 16th.

A full copy of the transcript from Ngo’s guilty plea proceeding is available here (PDF).

Tags: Arnold H. Huftalen, Court Ventures, Experian, findget.me, Hieu Minh Ngo, Senator Claire McCaskill, superget.info, Susan Henson, Tony Hadley, U.S. Secret Service, US Info Search

This entry was posted on Monday, March 10th, 2014 at 12:07 am and is filed under A Little Sunshine, Data Breaches, The Coming Storm. You can follow any comments to this entry through the RSS 2.0 feed. Both comments and pings are currently closed.