Identity theft victims face months of hassle

December 14 2014, byBrandon Bailey

In this Dec. 2, 2014 file photo, identity theft victim Mark Kim poses for photos in front of a Target store, in the Brooklyn borough of New York. Kim spent seven months trying to clear his credit history after his personal information was compromised in a data breach at Target last year. (AP Photo/Richard Drew)

As soon as Mark Kim found out his personal information was compromised in a data breach at Target last year, the 36-year-old tech worker signed up for the retailer's free credit monitoring offer so he would be notified if someone used his identity to commit fraud.

Someone did. The first monitoring report showed crooks opened accounts in his name at Macy's and Kohl's department stores, where they racked up more than $7,000 in charges. "My heart basically sank," he said. Over the next seven months the New York City resident spent hours on the phone, most of a day in a police station filing a report, and countless time sending documents to banks and credit reporting agencies to clear his credit history.

He's hardly alone. The Target hack during last year's Black Friday shopping weekend was just one in a wave of data breaches that have exposed more than 100 million customer records at U.S. retailers, banks and Internet companies. The latest high-profile hack, at Sony Pictures Entertainment, resulted in Social Security numbers and other personal details of nearly 50,000 current and former Sony employees and film actors being stolen and posted online for anyone to see. While cases are difficult to trace, analysts at Javelin Strategy & Research estimate that one in three Americans affected by a data breach ultimately became the victim of fraud last year—up from one in nine in 2010.

Although banks often absorb bogus charges, it's up to victims to clean up their credit histories and recover stolen funds. On top of lost time, money and emotional energy, victims face the frustration of rarely seeing anyone pay for the crimes. Identity theft cases are rarely prosecuted, said Avivah Litan, an analyst who studies fraud and identity theft for the research firm Gartner. Local police have limited resources, and criminals are often overseas, "so unless it's part of a bigger pattern, they're not going to spend much time pursuing it." Kim said a police detective who took his complaint later told him the accounts were opened by someone in California, but Kim never heard any more about the investigation.

In the past year, Target and other major retailers have said they're increasing security. President Obama has urged banks and stores to

speed up adoption of "chip-and-pin" payment cards, which are harder to hack. But reports of data breaches continue. And as Federal Trade Commission member Terrell McSweeney said recently, "Disturbingly, the news has seemed to desensitize many people to the real risks created each time an event occurs."

Kim can't be certain Target was the source of the fraud he experienced, he acknowledged. Experts say crooks often steal or buy consumer information from more than one source, and use it to compile a complete dossier on potential victims. That's likely the way hackers last year impersonated the rich and famous to get credit reports on Paris Hilton, Michelle Obama and even General Keith Alexander, then-head of the National Security Agency.

Alexander told a public forum this fall that when he tried to file his taxes, he learned someone else had already claimed a $9,000 refund in his name. Fraudsters also used his identity to apply for about 20 credit cards. The FBI eventually caught a suspect, he said; the FBI declined comment.

In this Dec. 11, 2013 file photo, then National Security Agency (NSA) Director Gen. Keith Alexander testifies on Capitol Hill in Washington. Alexander told a public forum this fall that when he tried to file his taxes, he learned someone else had already claimed a $9,000 refund in his name. Fraudsters also used his identity to apply for about 20 credit cards. (AP Photo/Manuel Balce Ceneta, File)

Meticulous by nature, Kim documented every conversation with an investigator or company representative. He was fortunate, he added, that his employer let him use the phone and fax machine where he works. "If I worked at a stricter company, it would have been a nightmare," he said. But Kim was never reimbursed for sending affidavits and other documents by certified mail to various banks and agencies.

While identity theft is certainly a global problem, experts say it's difficult to measure worldwide losses. However, a Department of Justice

study estimates identity theft of all kinds was responsible for U.S. financial losses of $24.7 billion in 2012—nearly double the $14 billion lost from all other property crimes such as burglary and theft. According to Javelin surveys in the U.S., when an existing credit card is exposed and then used for fraud, the average loss is $1,251. When a social security number is exposed and then used to open new accounts, the average loss is $2,330.

Banks take the biggest financial hit, but identity theft victims' out-of-pocket losses can range from an average of $63 for misuse of credit cards to $289 for fraud involving social security numbers. Of course that doesn't quantify lost time and stress.

Albert, who didn't want his last name published because he fears being victimized again, learned in 2012 that his personal information was exposed by a data breach at University of Miami Hospital, where he'd gone for minor surgery. After submitting his federal tax return the following year, the 60-year-old Miami resident found the government had already issued a refund to someone else using his social security number.

It took eight months for the airline reservations employee to get his $4,000 refund, which he needed to pay off debts. Albert said he doesn't know if the tax scammer used personal information from the hospital breach or some other source. But experts say health records are a treasure trove for scammers, since they may contain financial information, insurance numbers and personal data that can be used to obtain drugs, medical services or other benefits.

Albert now subscribes to a credit monitoring service and has asked reporting agencies for a "freeze" to block any applications for credit in his name. However, that "freeze" required a laborious process to lift when he later applied for a mortgage and then Internet service from

AT&T. He still worries someone will claim the Social Security benefits he's counting on when he retires.

"There's a rage that comes up, when you realize what happened," he said. "You feel violated. You feel attacked."

Kim just got all of the fraudulent accounts removed from his credit history this month. He and other victims say the experience has made them even more careful about their financial data and credit records. Kim, for example, registered for a security alert from the major credit reporting agencies, which advises lenders to contact him if someone tries to get credit in his name.

The alert expires in seven years, but Kim said he "absolutely" plans to renew it.

"I have to be watchful," he added. "I know something else could happen."