KPMG

Synthetic identity fraud: A $6 billion problem

As the fastest-growing financial crime in the United States, synthetic identity fraud bears a staggering $6 billion cost to banks.[1] To perpetrate the crime, malicious actors leverage a combination of real and fake information to fabricate a synthetic identity, also known as a "Frankenstein ID."[2]

It's no secret that data breaches are increasing in prevalence—in fact, this year's number of breaches could be record-breaking, according to a report by the Identity Theft Resource Center.[3] Fraudsters have taken advantage of this recent surge to obtain exposed personally identifiable information (PII), such as Social Security numbers (SSNs). Accompanied by a false name, address, and date of birth, these stolen SSNs can be used to apply for and build credit.

While the first application is typically rejected, this request creates a credit profile associated with the synthetic identity, legitimizing it from the perspective of other institutions. Repeated applications eventually lead to success for the fraudster, allowing them to secure lines of credit that they never intend to pay back.

Some immediately cash out on this opportunity, but oftentimes, there's a long play in which the fraudster will use the account responsibly to slowly increase their credit limit. In time, they'll enact a "bust-out" and proceed to max out the line of credit, abandoning the identity and leaving creditors with the responsibility of writing off the loss. This charge-off, on average, amounts to $15,000.[4]

Lenders, however, are not the only victims of synthetic identity fraud. The people who the stolen SSNs belong to experience ramifications, with many of these victims being children; a study by Carnegie Mellon's CyLab found that children's SSNs are 51 times more likely to be used in synthetic identity theft.[5] Other individuals who are unlikely to check their credit reports, such as the elderly and homeless populations, are also recurring targets.

The ability to create an unlimited number of identities, coupled with how challenging they are to detect, makes synthetic identity fraud a popular choice among cybercriminals. But despite its growing rate, synthetic identity fraud remains nearly impossible to flag during the application process.

If you're interested in finding out why, check out the next installments of this series, where we'll dive into what makes synthetic identity fraud so difficult to detect and how artificial intelligence and machine learning can be applied to detect this type of fraud.

[1] Synthetic Identify Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors, The Federal Reserve, July 2019.

[2] Synthetic Identity Fraud—The Frankenstein of Identity Theft, Experian, October 2019.

[3] Notified—The ITRC's Convenient, Comprehensive Source for Data Breach Information, Identity Theft Resource Center, 2021.

[4] Synthetic Identify Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors, The Federal Reserve, July 2019.

[5] Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers, Carnegie Mellon CyLab, 2011.

Contact us

Matt Miller
Principal
Cyber Security Services
KPMG LLP
T: 212-954-4648
E: matthewpmiller@kpmg.com

Ryan Budnik
Director,
Cyber Security Services,
KPMG LLP
T: 512-320-5200
E: rbudnik@kpmg.com

Sophia Chen
Associate
Cyber Security Services
KPMG LLP
T: 302-357-1747
E: svchen@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.