How synthetic identity fraud evades detection

In the first installment of this series, we detailed what synthetic identity fraud is and why we should care about it. As a quick summary, synthetic identity fraud occurs when cybercriminals create identities using a combination of real and fake information. These identities are commonly used to obtain loans without the intention of paying lenders back.

Its difficulty to detect has quickly established synthetic identity fraud as a leading crime, costing banks more than $6 billion total or $15,000 per occurrence in damages. In this article, we’ll discuss what makes this type of fraud a challenge to detect.

When you apply for credit, a few key pieces of information are required. These include your Social Security number (SSN), name, date of birth, and address, among others. With this information, lenders can pull a credit history to assess your risk and ultimately determine whether they’ll grant you a line of credit. In some instances, individuals may have limited credit history or are rebuilding their credit—fraudulent applications frequently resemble these situations.

But what about verifying that the SSN provided matches the name, address, date of birth, and other personally identifiable information (PII) provided? We would think that this process is straightforward. However, there isn’t an efficient method to electronically validate that the PII provided is associated with that particular SSN. The current method is too time-consuming when verdicts on applications are often provided within minutes of submission.

Furthermore, in 2011, the Social Security Administration began assigning random SSNs to “protect the integrity of SSNs and to extend the pool of nine-digit SSNs available nationwide.” This is in contrast to when SSNs were issued following a clearly defined numbering scheme. The nine-digit number was composed of three parts: the Area Number, the Group Number, and the Serial Number. Under this scheme, we could check whether the address, for example, is plausible based on the SSN provided as the Area Number is assigned based on geographical region. This type of analysis is not possible with the new randomization strategy.

Instead of assessing applications holistically, institutions may instead rely on validating each piece of information individually—this means that if the name, address, date of birth, and SSN are valid on their own, banks are none the wiser.

Equipped with this background, we may now ask ourselves: What can we do to detect synthetic identity fraud? The final installment of this series aims to answer this question, exploring how artificial intelligence and machine learning can be applied to combat this type of fraud.

---

2 Ibid.
3 Social Security Numbers, Social Security Administration, 2021.
Contact us

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

Chadd Carr  
Director  
Cyber Security Services  
KPMG LLP  
T: 703-286-8565  
E: chaddcarr@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.

© 2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. NDP275691-1B