How Synthetic Identities are Used to Defraud the Banking Industry and How to Stop it

Lukayn Hunsicker and Deleep Nair
July 23, 2020
Learning Objectives

- Understand just how prevalent application fraud and synthetic identities are, what it looks like and what to put in place to avoid it

- Discuss real-world scenarios where such activity took place and the impacts it had on banks

- Identify tools available to Banks such as analytics, watch lists and third party data
Agenda

- What is a Synthetic Identity?
- How are Synthetic Identities created?
- The impact of Synthetic Identity Fraud on industry
- Tactics to identify a Synthetic Identity
- How can we combat Synthetic Identity Fraud
Speaker Bios

Lukayn Hunsicker, Global Head - Banking Fraud Product Management, BAE Systems Applied Intelligence
Lukayn is the Global Head of Banking Fraud Product Management for BAE Systems Applied Intelligence. He serves as a subject-matter expert in the areas of financial crime and fraud, delivering and maintaining fraud prevention solutions of value for BAE System’s diverse global customer base. He has over 15 years of experience in the financial services and software industries. In addition, he has held product consulting roles pertaining to cybersecurity, cyber-enabled crime and risk. LinkedIn: https://www.linkedin.com/in/lukayn-h-3646319/

Deleep Nair (CFE), Global Financial Crime Analytics Lead, BAE Systems Applied Intelligence
Deleep is the Global Financial Crime Analytics Lead for BAE Systems. Deleep is an experienced Data Scientist and Project Manager with strong experience leading cross-disciplinary teams in planning and developing end-to-end fraud analytic solutions. He has worked with large government agencies to develop analytic solutions for fraud and contraband detection. Deleep has deep interests in combining analytics with fraud detection and is a member of the American Statistical Association and a Certified Fraud Examiner. LinkedIn: https://www.linkedin.com/in/deleep-nair-cfe-89322617/
What are Synthetic Identities?

The generally agreed-upon definition of synthetic identity fraud is a crime in which perpetrators combine fictitious and sometimes real information, such as SSNs and names, to create new identities to defraud financial institutions, government agencies or individuals.
Synthetic Id Fraud Vs. Traditional Id Fraud

DIFFERENTIATING TRADITIONAL IDENTITY FRAUD FROM SYNTHETIC IDENTITY FRAUD

Traditional Identity Fraud
- Perpetrator
- Person A’s name
- Social Security
- Person A

Legitimate Use
- Person A
- Social Security
- Person A
- This is a real person who uses valid information to set up accounts and obtain credit.

Synthetic Identity Fraud
- Perpetrator
- Fake name
- Other fake identifying information
- Social Security
- Person A
- Synthetic ID
- Person A
- This is a fraudster who combines fake and sometimes, real information to establish a credit record under the new synthetic identity.

How are SIs Created

Credit Applications
- Fake or real SSN is combined with other PII
- Fraudster applies for credit and is denied
- Credit file created using the fake credentials
- Apply again for low limit card and get approved

Authorized User
- Added on as an authorized user to an existing account with good credit
- Credit history retained even after Synth. ID removed
- Card owners are recruited as pollinator accounts

Data Furnishing
- Front Company created and approved by CRAs to provide payment history (Car Dealerships, etc.)
- An "applicant" applies for credit for a fictitious purchase of the business’s product
- Each month, the business reports payments on the credit account associated with the synth. id
Dark Web and SIs

- Results from Dark Web search for fake passport and fake ID search
- TOR anonymizes location and identity of people accessing these websites
- “Reputation” of these websites is very important to their business model
- Many sites will go through extensive “vetting” to ensure you are not law enforcement before rendering service
High Security
Our client's security is our number one priority. 100% SECURITY is guaranteed to all our clients. We keep all our clients encrypted for a period no longer than 1 month after we ship out our clients' orders, after which all the information will be deleted from our server.

High Materials
Genuine sophisticated materials are used for the production of the documents. We use the same quality materials used by government authorities worldwide so as to bring the most secure, durable and quality products to our clients who used our documents. Thus, all our products are of 100% quality.

Fast Shipping
Shipping is usually done using either FedEx, UPS, USPS or DHL, depending on your location in the world. Average shipping is 3 days, but it can take up to 7 days for some countries.

Scannable Documents
Our real documents can pass any test including data scanning devices. You can be confident going through customs with our real passports; we guarantee nobody will stop you at the border because your documents are genuine.

Biometric Data Registration
We do provide top quality and secure biometric registration for our documents. We may require information such as your fingerprints in order to complete your registration into some government databases. So if needed, your biometric information can be easily accessed and verified.

Data Verification
Any government official can verify your real documents bought online. You can also do it yourself by using the government website, Tepoint code or a verification diskette that we give to every client.

Confidentiality
We guarantee a 100% confidentiality for all inquiries and orders made by our clients. For this reason, we make sure all transactions and discussions are through secure lines and application.

Durability and Guarantee
Our documents are accepted globally and are very authentic. So clients will be able to travel and stay in other countries safely. We also offer durability guarantees for all purchase done through us.
Our Firm

We are the Best, Reliable and Most Recommended makers of High-quality Fake and Real archives, every one of our records are searchable and will pass all security checks, Registered in the database same day: Passports, drivers licenses, ID cards, Social security card, birth authentications, Concealed Carry Weapon Permits (CCW), Federal Firearms License (FFL), confirmations, Visas, SSN, Marriage declarations, separate papers, US green cards, University degrees, Money, SSD compound arrangement and actuation powder utilized for cleaning covered dark cash, and different reports for various nations: USA, Australia, Belgium, Brazil, Canada, Italy, Finland, France, Germany, Israel, Mexico, Netherlands, South Africa, Spain, United Kingdom. This rundown isn't full for more data and the procedure.

Our Customers...

we are the best that what our customers say about us if you can’t believe this then you can check the testimony page. If you need our work samples then just you need to do is ask us that’s it and we will send you the samples. our work and process is the safest one where you get the most desired result within a reasonably priced tag and timeline.
### Impact of SIs

<table>
<thead>
<tr>
<th>Category</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of children who were victims of SI fraud in 2017</td>
<td>1M</td>
</tr>
<tr>
<td>SI fraud cost to Financial Institutions</td>
<td>$6 B</td>
</tr>
<tr>
<td>Applicants identified as potential SIs not detected by Fraud Systems</td>
<td>85% - 95%</td>
</tr>
<tr>
<td>Percent of credit losses due to synthetic identities</td>
<td>20%</td>
</tr>
<tr>
<td>PII Records exposed</td>
<td>446 M</td>
</tr>
<tr>
<td>Percent of tax returns that appeared to be for SIs</td>
<td>1.4%</td>
</tr>
<tr>
<td>Average loss due to SI Fraud</td>
<td>$10K</td>
</tr>
<tr>
<td>Percent of applicants with SIs using digital channels</td>
<td>50%</td>
</tr>
</tbody>
</table>
Impact of Synthetic Identities

• On January 5, 2017, Robert F. Dixon, Jr., of Chamblee, Georgia, was sentenced to two years, ten months in federal prison to be followed by three years of supervised release for wire fraud conspiracy, wire fraud, and misuse of a Social Security number. Dixon was ordered to pay restitution in the amount of $403,734.55.

• On November 17, 2016, Karen A. Bradley, of Lithonia, Georgia, was sentenced to one year, six months in federal prison to be followed by three years of supervised release for wire fraud conspiracy and misuse of a Social Security number. Bradley was ordered to pay restitution in the amount of $244,232.31.

• On September 1, 2016, Landerick C. Mitchell, of North Charleston, South Carolina, was sentenced by U.S. District Judge Leigh Martin May to six months in federal prison to be followed by three years of supervised release for wire fraud conspiracy and misuse of a Social Security number. Mitchell was ordered to pay restitution in the amount of $23,328.86.

• On January 10, 2017, Maurice R. Lambert, of Atlanta, Georgia, pleaded guilty to access device fraud and misuse of a Social Security number. He is scheduled to be sentenced by U.S. District Judge Eleanor L. Ross on May 25, 2017.

Impact of Synthetic Identities - Largest Synthetic Identity Crime Ring

- 18 criminals were charged by the US Justice Department for running the most sophisticated Synthetic Identity crime rings in history.
- Together they created 7,000 new identities, applied for and received 25,000 separate credit cards and had them sent to 1,800 different addresses.
- They managed to steal at least $200 million in a three-step process they repeated thousands of times:

  **Make up** a false identity by creating fraudulent identification documents and a fraudulent credit profile with the major credit bureaus.

  **Pump up** the credit of the false identity by providing false information about that identity’s creditworthiness to the credit bureaus. Believing the furnished information to be accurate, the credit bureaus would incorporate this material into the false identity’s credit report, making it appear that the false identity had excellent credit.

  **Run up** large loans using the false identity. The higher the fraudulent credit score, the larger the loans that the defendants could obtain. These loans were never repaid, and the defendants reaped the profits.

Where Do We See SIs in Banking?

Application Process:

A Synthetic Identity is particularly difficult to recognize as some of the information submitted is valid and will go undetected creating a greater chance of obtaining credit.

Disruption of Customer Lifecycle:

A Synthetic Identity can be utilized as an authorized user post ATO attack – giving the fraudster access to additional funding prior to bust out actions.

Additionally, expect a rise in Muling activity as P2P activity increases.
Why are SIs So Hard to Catch in Banking?

- The information appears correct (some of it is) and the criminal looks like a regular customer
- Payments made on time
- Alternately, when an SI ultimately goes delinquent collections teams will be chasing ghosts
- The person whose information was stolen is not aware so it has not been reported
- Single validation tool may not detect red flags such as SSN / DOB mismatches
- Low staffing/ short investigation time/ internal SLAs
- Lack of experience or training
How can you detect SIs?

- Better Controls in Place
- Link Analysis
- Specialized SI models
  - Behavior Analytics
  - 3rd Party Data
How can you detect SIs – Risk Controls

• Stronger Fraud Risk Controls

• Ensure that FIUs are trained in catching the elements of SI fraud

• Ensure investigators are aware of SI fraud typologies and how it can be manifested in credit/debit and loan products
  o Credit file depth is inconsistent with customer age or other profile information
  o Multiple identities with the same SSN
  o Multiple applications from the same phone number, mailing address or IP address
  o Use of secured credit lines or piggybacking to build credit
  o SSN issued after 2011
  o Multiple authorized users on the same account

• Utilize Consent-Based Social Security Number Verification (eCBSV) once it is rolled out (June 2020)
How can you detect SIs – Link Analysis

• Experts identify link analysis as effective in catching networks of SIs across financial products
• Identifying multiple users/customers with the same SSN or same address/contact information
• Link across products to discover commonalities between entities
• Capable entity resolution
How Can you Detect SIs – Specialized AI models

- Unmatched depth and consistency of credit file
- Multiple account applications from the same IP address
- Use of hotkeys/autofill and other digital entry techniques
- Depth/Consistency scores
- 3rd party verifications scores/databases of suspected SIs

Recommendations

We propose three key areas to focus on if you’re seeking to ward off potential fraudsters and keep genuine customers happy:

1. **Investment** – Internal processes and technology should be bolstered to improve the identification of suspect cards/loans at the application stage and reduce the chance of fraudulent charge offs (limiting financial losses).

2. **Intelligence** – Better identify patterns across applications from individuals or devices.

3. **Risk** – Use wider industry data, intelligence and information to more accurately (and quickly) identify risk.
Questions?
Contact us

E: learn@baesystems.com


Unpublished Work Copyright © 2020 BAE Systems. All Rights Reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc.

The information in this document contains proprietary information of BAE Systems. Neither this document nor any of the proprietary information contained therein shall be (in whole or in part) published, reproduced, disclosed, adapted, displayed, used or otherwise made available or accessible (in each case, in any form or by any means) outside of BAE Systems without the express written consent from the document originator or an approved representative of BAE Systems.