The New Reality of Synthetic ID Fraud

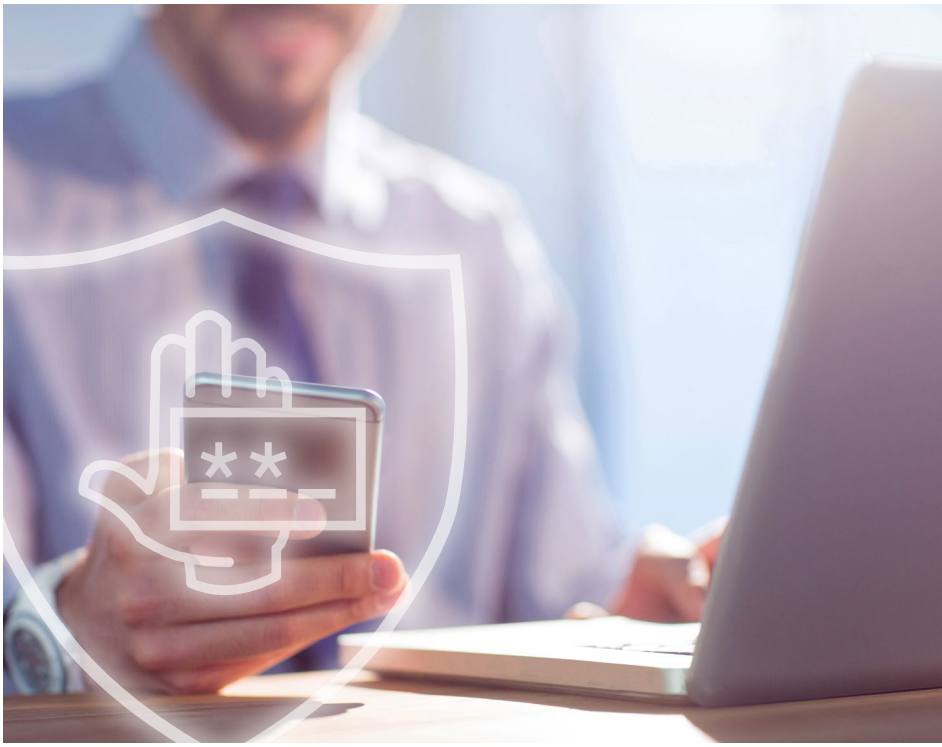
How to Battle the Leading Identity Fraud Tactic in The Digital Age

EQUIFAX®

In the 15 years since synthetic identity fraud emerged as a significant threat, it has become the predominant tactic for fraudsters. The trend is not likely to slow.

As organizations get better at fending off point-of-sale fraud tactics, fraudsters are expected to focus more of their activities on new-account fraud, often with bogus identities. Javelin Strategy & Research estimated that new-account fraud will soar 44% between 2014 and 2018, rising from $5 billion in annual losses to a projected $8 billion.[1]

This white paper examines why synthetic ID fraud is becoming a go-to tactic for highly organized fraudsters and how organizations can mitigate the risk more effectively.



[1] Javelin Strategy & Research, *2015 Data Breach Fraud Impact Report*, June 2015

Synthetic ID Fraud: A Short History

Synthetic ID fraud is built on the foundation of a fictitious identity, often created with a combination of real data and fabricated information. For example, the fraudster may "borrow" one person's Social Security number (SSN), combine it with another person's name, and use someone else's address to create a brand new identity. The perpetrator can then use this fraudulent identity to apply for credit, make major purchases, or a variety of other activities that give the identity a financial history.

Today, synthetic ID fraud accounts for 80% of all credit card fraud losses, and nearly one-fifth of credit card charge-offs.

Source: InformationWeek

Historically, synthetic ID fraud was generally committed by consumers whose poor credit ratings made it difficult to open credit card accounts or receive loans. With a few adjustments to their personally identifiable information, cash-strapped consumers were able to create new accounts. Synthetic ID fraud has since transitioned into a widely used criminal activity designed to steal many millions of dollars. For example, in 2013 the U.S. Attorney's Office for the District of New Jersey charged 18 defendants with plotting a $200 million credit card fraud conspiracy that involved fabricating more than 7,000 identities to obtain tens of thousands of credit cards.[2]

Today, synthetic ID fraud accounts for 80% of all credit card fraud losses, and nearly one-fifth of credit card charge-offs. The value of refunds over the past three years to cover those charge-offs has reached $20 million.[3]

In Canada, individual fraudulent credit card applications resulted in an average loss per account of $2,003.61 in 2013.[4] Numbers are similar in the U.S. and across Europe.

---

[2] Federal Bureau of Investigation, "Eighteen People Charged in International $200 Million Credit Card Fraud Scam" (press release), Feb. 5, 2013

[3] InformationWeek, "Synthetic Identity Fraud A Fast Growing Category," Oct. 21, 2014

[4] Canadian Bankers Association, "Credit Card Fraud and Interac Debit Card Statistics - Canadian Issued Cards," https://assets.documentcloud.org/documents/1684634/canadian-bankers-association-credit-card-fraud.pdf

Why Synthetic Fraud ID

The rise in synthetic ID fraud can be attributed to a variety of conditions. First, it's not especially difficult to create a synthetic ID. The steps include:

- Obtain an SSN of another person
- Fabricate a name to be used with the SSN
- Create false birth dates that tend to match the appearance of the fraudster in case any in-person appearances are required
- Create an address to receive mail fraudulently
- Provide telephone numbers that will probably be untraceable or stale by the time the fraud is realized

Once the identities are created, fraudsters typically nurture them until they mature. They open accounts at different organizations, check their credit scores regularly, and choose the perfect time to exploit the accounts to the maximum degree possible. In the aftermath, financial-services organizations are generally left with a significant loss and nobody to chase in their collection and recovery process.

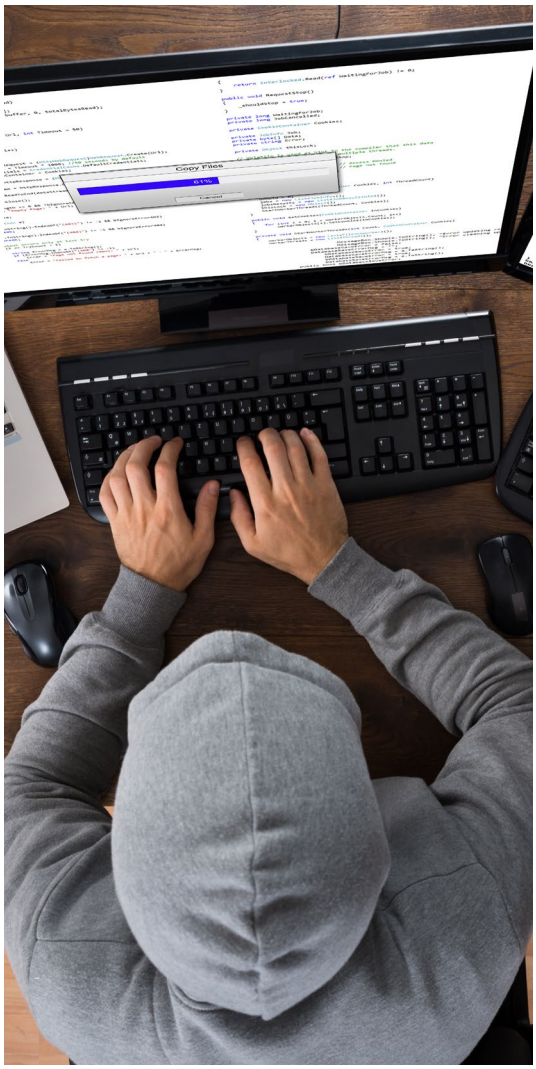
Fraudsters have relatively easy access to personally identifiable information to create synthetic ID facilities. Data breaches, often massive, are a primary source.

In the digital age, obtaining verifiable data to create a synthetic ID and nurture it is becoming increasingly easy. Making matters worse is that financial institutions may not have best-practice processes in place to verify an applicant's information.

Further, the fail-safes for many fraudulent activities are not in place with synthetic ID fraud. Since real people won't see activity on an account created with their SSN that doesn't include their exact name or address, they're not going to raise any red flags. And when unusual activity does occur on the fake account, the synthetic-identity fraudster will promptly confirm that the suspicious activity is "legitimate" if contacted.

Fraudsters have relatively easy access to personally identifiable information to create synthetic ID facilities. Data breaches, often massive, are a primary source. (See "Data Breaches and Synthetic ID Fraud")

While the ease of creating a synthetic ID has prompted more fraudulent activity, the potential "take" for related activities is equally compelling. With patience possibly being their only virtue, synthetic ID fraudsters often invest long periods of time to increase the value of their scams. (See "7,000 Fake IDs, $200 Million In Real Losses")



Data Breaches and Synthetic ID Fraud

The building blocks of a synthetic ID can include personally identifiable information (PII), but the opportunities for fraud that Social Security numbers (SSNs) provide make them highly valuable for fraudsters. More than 65% of top financial institutions allow the use of SSNs as identifiers.

Javelin Strategy & Research projects that the number of victims of an SSN breach that experience fraud in the same year will grow nearly 45%, from 500,000 in 2014 to 710,000 in 2018.[5]

Those figures are relatively low considering the number of SSNs that are exposed through data breaches. In 2015 alone, a number of significant breaches gave fraudsters access to millions of SSNs.

For example, breaches at two major health insurance companies exposed SSNs, birth dates and other account data of more than a combined 91 million subscribers.[6]

Two breaches at the Office of Personnel Management revealed the personal data of more than 22 million current and former federal employees. In July, a breach of the Army National Guard exposed the Social Security numbers of 850,000 current and former National Guard members.[7]

To avoid possible detection, fraudsters often seek out SSN of people who don't make use of credit. The elderly are targeted, especially those living with relatives who are less likely to use credit cards or pay utility bills.[8] Children are targets, too, primarily because parents are extremely unlikely to check their credit reports, which limits fraud detection.

---

[5] Javelin Strategy & Research

[6] CRN.com/The Channel Co., "The 10 Biggest Data Breaches of 2015 (So Far)," July 27, 2015

[7] *Ibid*

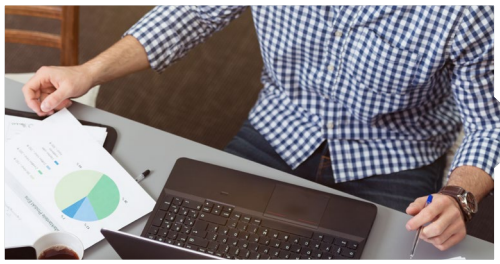
[8] Creditcards.com, "Synthetic Identity Theft Crimes Growing Fast, Targeting Kids," April 24, 2015

Combating Synthetic ID Fraud

The increasing capability of digital technology to swiftly review massive databases enables organizations to recognize fictitious identities as they are being created or used for fraudulent purposes.

Proprietary algorithms in robust solutions are especially useful in identifying synthetic IDs. By comparing an SSN to a consumer's unique identification information, the algorithm determines how well a consumer's SSNs matches its identity.

The most useful tools return both positive confirmations of an SSN match and several negative alerts that can signal the creation of a synthetic identity or other SSN-related fraud at account opening — before any damage is done. This added assurance is important when establishing new relationships and can also be a valuable part of a red flag compliance program.



Proprietary algorithms in robust solutions are especially useful in identifying synthetic IDs.

Warnings to look for:

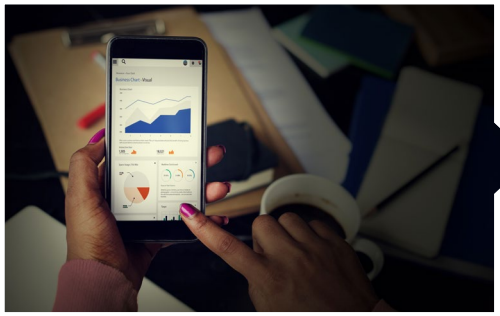
- SSN can't be matched to the specific consumer based on comparison algorithms
- SSN matches to a different consumer, while no credit file is available for the requested applicant
- SSN matches to different consumer, and a credit file is available for the name and address provided; however, the SSN on that file is different from the SSN provided on the inquiry.

Discover Suspicious Patterns with Advanced Analytics

Additional analytics-based solutions can combat synthetic ID fraud by delivering insight that detects linkages and suspicious patterns, which help determine that the applicant is a real person.

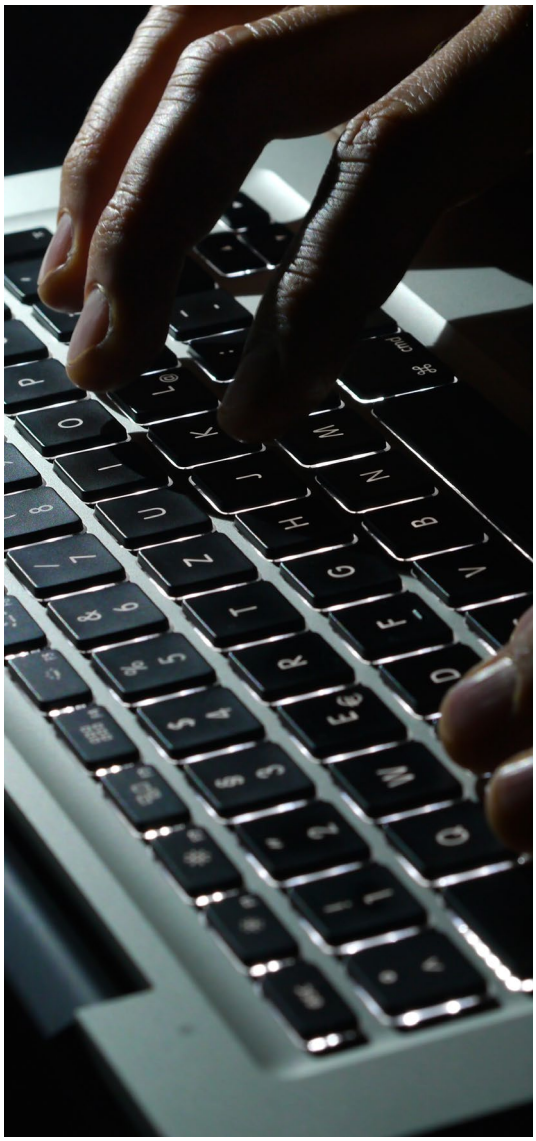
These models leverage advanced keying logic to validate components of an applicant's identity beyond an SSN. Keying technology drives down the number of false positives that normally accompany fraud products. Equifax customer studies show that decisions based on high-quality data about an individual from multiple data assets and advanced analytics can cut false positives by as much as 25%.

The most sophisticated solutions provide information that helps determine if there are inconsistencies with the applicant's behavior across a consortium of data or if the application has high-risk variables that are known to be predictive of fraud.



Additional analytics-based solutions can combat synthetic ID fraud by delivering insight that detects linkages and suspicious patterns, which help determine that the applicant is a real person.

Unique data assets provide the most predictive fraud score, tailored specifically to a company's business needs. Verified, non-public data can help organizations identify up to 99% of their user populations.



7,000 Fake IDs, $200 Million In Real Losses

In 2013, federal authorities shut down a massive synthetic ID fraud scheme that created 7,000 false identities to obtain more than 25,000 credit cards that resulted in more than $200 million in confirmed losses.[9]

The scheme involved a three-step process that included:

- Fabricating synthetic identities by creating fraudulent identification documents and credit profiles
- Boosting the credit of the synthetic identities by providing false creditworthiness information
- Running up large loans using the false identity

To remain undetected, the fraudsters maintained more than 1,800 "drop addresses," including houses, apartments and Post Office boxes, which were used as the mailing addresses of the false identities.

They also created dozens of sham companies that did little or no legitimate business, obtained credit card terminals for the companies, and then ran up charges on the fraudulent credit cards.

The Federal Bureau of Investigation commented that the scheme generated enormous profits for the defendants. To support the scheme, the fraudsters reportedly spent millions of dollars sustaining the elaborate network of drop addresses and running credit reports on the thousands of false identities.

The goal was "to get credit cards, get the credit limits as high as possible, then use those credit limits to max them out, and then walk away, said U.S. Attorney Paul J. Fishman.[10] "A lot of what they did was very painstaking and very sophisticated and took a long time."

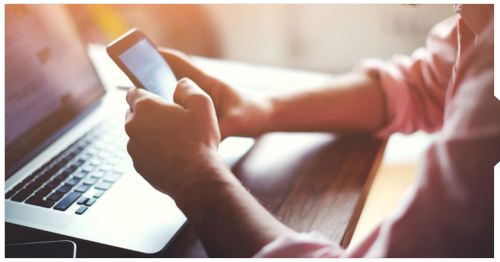
[9] Javelin Strategy & Research

[10] FBI, Feb. 5, 2013

Summary

The growth of synthetic ID fraud shows few signs of slowing. Easy access to data that fraudsters use to create synthetic IDs will continue to make fraud an attractive option for them.

Fortunately, robust and reliable countermeasures to synthetic ID fraud are available to organizations. With these solutions, organizations can quickly, reliably and affordably identify suspicious activity to help mitigate risk without encumbering legitimate consumers with unnecessary checks.



Robust and reliable countermeasures to synthetic ID fraud are available to organizations.

Need more information on how you can mitigate the risk of synthetic ID fraud? Equifax can help you understand how advanced fraud detection solutions can recognize the warning signs of synthetic ID fraud to take appropriate action early.

CONTACT US TODAY

For more information:
1-877-262-5261
equifax.com/business/prevent-fraud