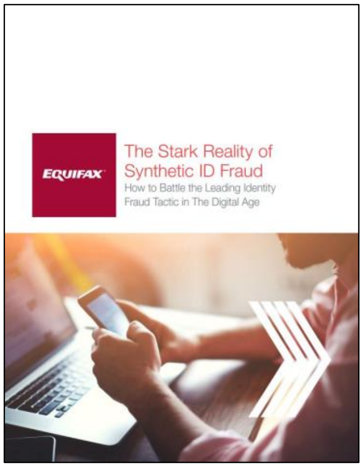

EQUIFAX
The Stark Reality of Synthetic ID Fraud
How to Battle the Leading Identity Fraud Tactic in The Digital Age

The Stark Reality of Synthetic ID Fraud

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

Thank you for downloading this Equifax whitepaper. Carahsoft is the public sector distributer for Equifax solutions available via NASA SEWP V, National Cooperative Purchasing Alliance (NCPA), NJSBA, and other contract vehicles.

To learn how to take the next step toward acquiring Equifax's solutions, please check out the following resources and information:

For additional resources:
carah.io/EquifaxResources

For upcoming events:
carah.io/EquifaxEvents

For additional Equifax solutions:
carah.io/EquifaxSolutions

To purchase, check out the contract vehicles available for procurement:
carah.io/EquifaxContracts

To set up a meeting:
Equifax@carahsoft.com
844-747-6222

For more information, contact Carahsoft or our reseller partners:
Equifax@carahsoft.com | 844-747-6222

The Stark Reality of Synthetic ID Fraud

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

Scoping Out Synthetic ID Fraud

In the 18 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 down.

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.

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. 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, synthetic ID fraud was found to be the basis of one of the FBI's largest credit card scams. A ring of 22 fraudsters, based in New York and New Jersey, apparently created fake identities and credit profiles, bolstered their creditworthiness with bogus information, and then went on spending sprees without repaying debts. The scam cost banks and other businesses more than $200 million in losses from 2016-17.[2]

That was just one case. According to data from Auriemma Consulting Group, synthetic ID fraud is responsible for 5% of charged-off accounts and up to 20% of credit losses – or $6 billion in 2016 alone.[3]

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

[2] Fortune Magazine, "Fraudster Surrenders in 1 of the FBI's Biggest Ever Credit Card Scams", January 25, 2017.

[3] Auriemma Consulting Group, August 2017

In 2017, Equifax conducted a study[4] of its credit card issuers processing more than 80 million new accounts per year. Results showed that just within a year's time, a half million accounts were identified as potential synthetic identities — an average of nearly 40,000 accounts per issuer with an average balance of $2,049. This translates to an average loss of more than $300 million to the credit card industry.

Why Synthetic ID Fraud

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

- 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

Synthetic ID fraud was estimated as a **$700M+** problem in 2016 in the US alone, growing at over **17%** a year.

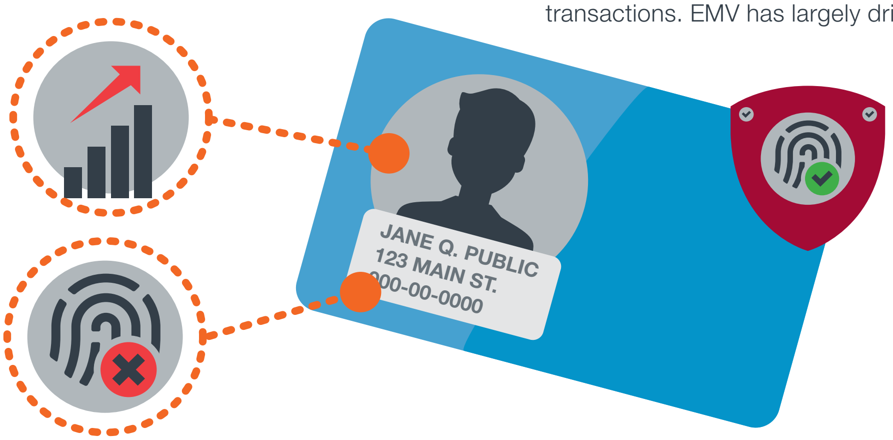
[4] Equifax Data Analysis, June 2016 – June 2017

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, organizations in industries like financial services and telecommunications/utilities are generally left with a significant loss and nobody to chase in their collection and recovery process.

In the aftermath, organizations in industries like financial services and telecommunications/utilities are generally left with a significant loss and nobody to chase in their collection and recovery process.

In the digital age, obtaining verifiable data to create a synthetic identity and nurture it is becoming increasingly easy. Once created, fraudsters can introduce the synthetic identity into the system by requesting a service or applying for loans/credit within a "faceless" channel. Making matters worse is that 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 identities. Data breaches, often creating a treasure trove of identity data, are a major contributing factor to synthetic ID fraud. Another contributing factor may be the rise of EMV (Eurocard, MasterCard, Visa) – cards that use computer chips to authenticate (and secure) transactions. EMV has largely dried up the opportunity for counterfeit card



schemes, instead shifting fraudsters to the application fraud, card-not-present and account takeover space.

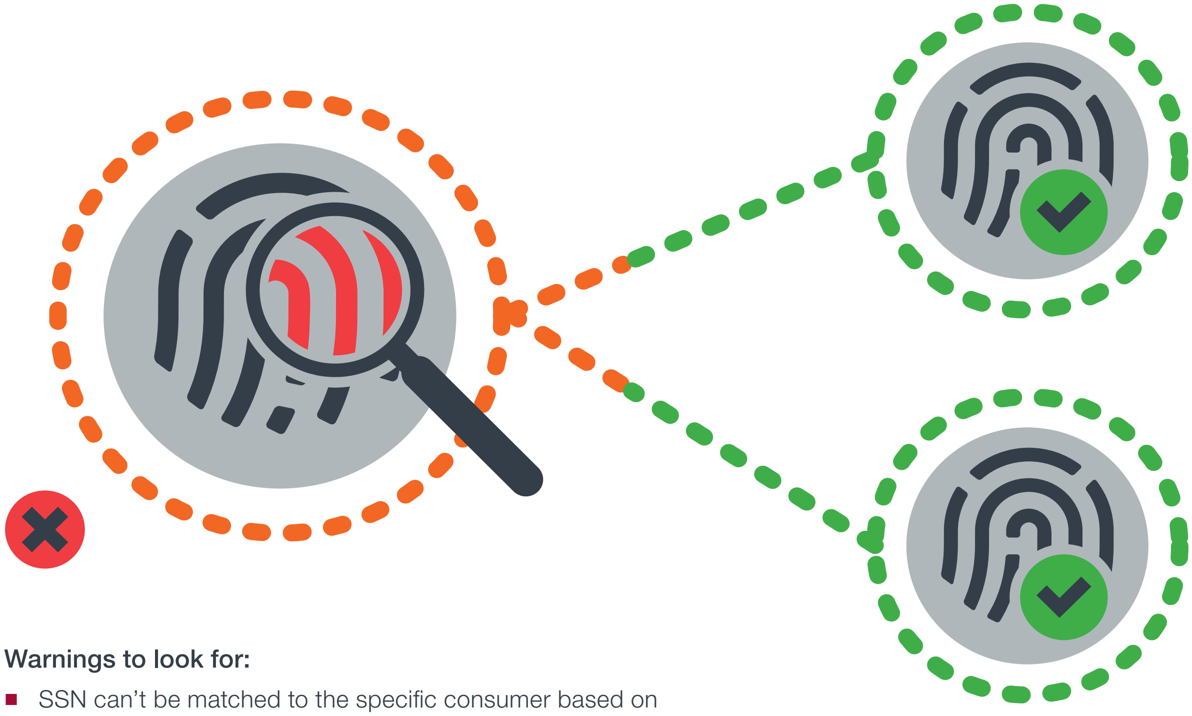
Proprietary algorithms in robust solutions are especially useful in identifying synthetic identities.

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 identities. By comparing an SSN to a consumer's unique identification information, the algorithm determines how well a consumer's SSN 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.



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 a 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 insights that detect 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 tools—such as a fraud score—that are tailored specifically to a company's business needs. Also, verified, non-public data can help organizations identify up to 99% of their user populations.

Algorithms that analyze attributes such as authorized user velocity and identity discrepancies are also useful in determining if the identity presented is potentially synthetic. An authorized user is someone who is granted access to another person's credit card account. Authorized users receive full access to the account's credit line, but are not legally responsible for paying the balance or associated fees that result from their use of the account. Once an authorized user is added to a credit card account, the issuer will begin relaying account information to the major credit bureaus on a monthly basis under the authorized user's name. As long as the account is managed well, the authorized user's credit report should reflect positive information, whereas account mismanagement (e.g., missing payments or exceeding the credit limit) produces the opposite effect. If the authorized user has no previous credit history, his or her first credit score should be generated within six months.

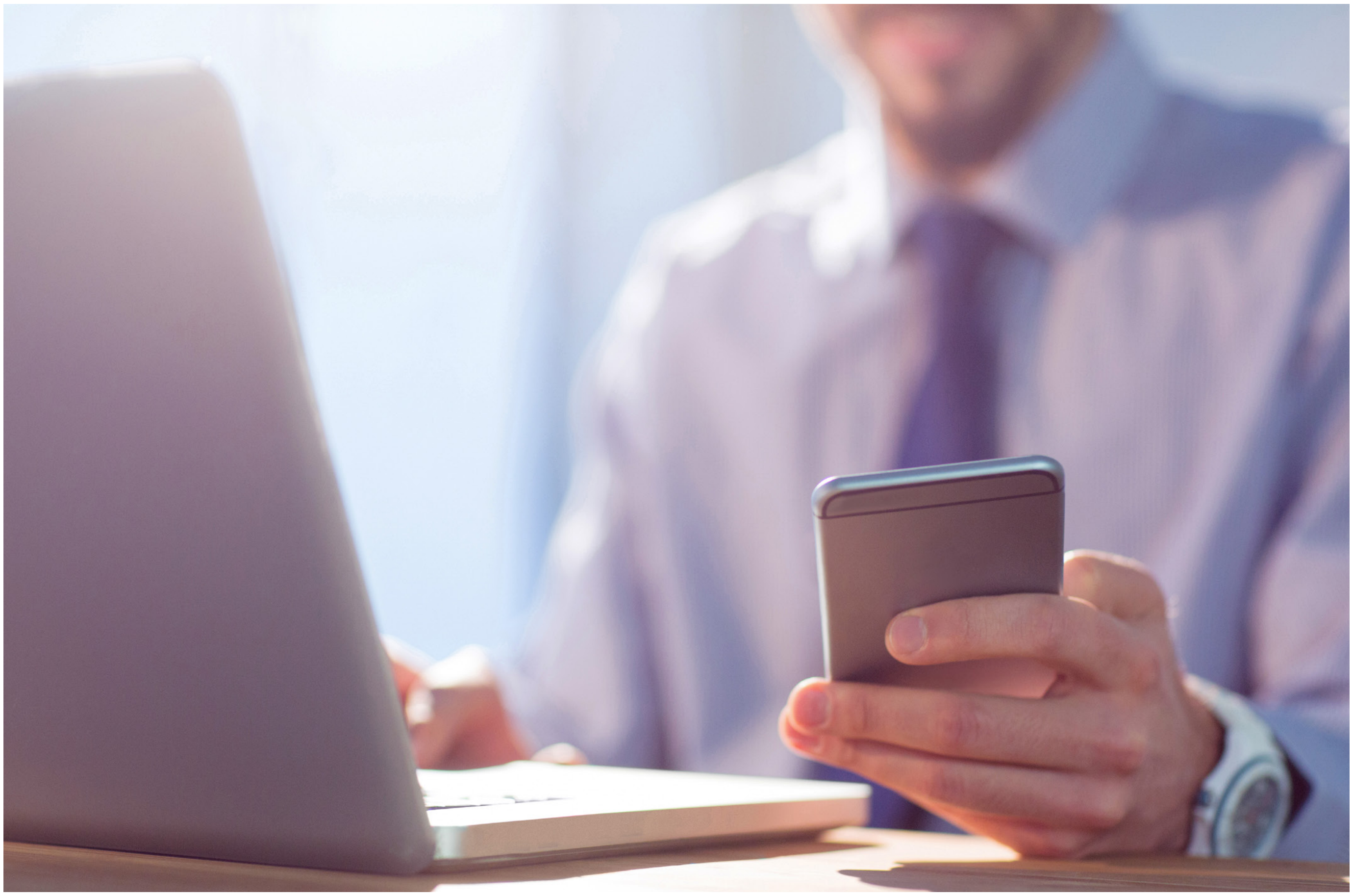
While the practice of adding authorized users may not be illegal, it can pose significant risks to financial institutions – leading to authorized user abuse. Sometimes called credit boosting or piggybacking, authorized user abuse occurs when low-risk primary card owners “rent” their tradelines with extensive credit histories, high credit limits and solid repayment profiles to others – most times, knowingly, to fraudsters. The synthetic scheme looks very similar to the appropriate use, which is why having analytics in place to detect this potential fraud is so critical.

Summary

The growth of synthetic ID fraud shows few signs of slowing. Easy access to data that fraudsters use to create synthetic identities 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.

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. Visit us online at www.equifax.com/business/prevent-fraud.



CONTACT US

1-877-262-5261
equifax.com/business/prevent-fraud