

DEFINING SYNTHETIC FRAUD

A SentiLink white paper published in support of industry and government groups' efforts to outline the hard-to-define problem of synthetic fraud.



EXECUTIVE SUMMARY

Synthetic fraud is the fastest growing form of fraud in financial services. Unlike identity theft, synthetic fraud generally lacks a consumer victim who would recognize fraudulent activity associated with their identity. Because the traditional feedback loop between customer and financial institution is broken and the problem of synthetic fraud is not well understood, financial institutions apply inconsistent nomenclature and disjointed detection mechanisms, resulting in wildly varying industry estimates of the size of the synthetic fraud problem.

Banks and lenders often attribute all unexplainable financial losses to synthetic fraud. Companies identify synthetics using credit behavior attributes, such as “charge off with no contact or payment and a card utilization rate above 75%” or a “never pay.” Some solution providers define synthetic fraud using a combination of consumer behavior, linkages, inquiry velocity, and credit performance—and generate scores based on those characteristics.

While there are differences in definitions and approaches to the problem, most agree on the following:

- ✓ Synthetic fraud is a hard-to-measure multi-billion-dollar problem that impacts financial services, healthcare, utilities, communications, and the payments industries, as well as the sharing economy.
- ✓ Synthetic fraud opens the door to bad actors who perform criminal activity, including money laundering and human trafficking.
- ✓ Synthetic identities can exist undetected for years and eventually bust-out, causing higher average loss amounts than traditional fraud.
- ✓ There are certain tactics used by synthetic fraudsters to create and strengthen synthetic identities and their associated credit histories, which include establishing new identities with the credit bureaus through credit inquiries, “piggybacking” on authorized user tradelines, acquiring “boosted tradeline” loans, performing “credit washing,” and leveraging non-reputable credit counseling services.
- ✓ Although the industry is working toward a common definition, “synthetic fraud” remains a catch-all term defined differently by solution providers, financial services companies, and regulators.
- ✓ Financial services companies, regulators, law enforcement, and solution providers want the ability to gather information on fraudsters and other bad actors who are perpetrating synthetic fraud, but compliance and reputational risks, operational costs, and blurred definitions inhibit effective data sharing.
- ✓ To best collectively combat the problem of synthetic fraud, industry and government leaders need to agree on a common definition of synthetic fraud.

This white paper is designed to help provide insight and fuel ideas and debate as the industry moves toward developing a broadly adopted standard for certain fraud definitions.

Defining Synthetic Fraud

We believe there are three principles to be followed as we collectively develop a definition:

1. Definitions should be unambiguous and avoid language that can inadvertently describe other forms of fraud.
2. Definitions should provide guidance for follow-on validation whenever possible.
3. Ancillary definitions for related frauds should be provided in order to clearly define synthetic fraud in relation to other fraud behaviors.

Having a consistent definition allows:

- Financial institutions to more accurately track instances of synthetic fraud over time.
- Industry and government groups to collect accurate data about the size of the synthetic fraud problem within and across industries.
- Data contributors to contribute helpful information more openly with lower reputational and compliance risks.
- Fraud solution providers to build models and propose verification flows that most accurately and efficiently addresses synthetic fraud behavior.
- Industry to request clearer interpretations or changes to existing regulations that are hindering the fight against synthetic fraud.
- Solution providers and fraud analysts to efficiently utilize various forms of verifications to detect synthetic applications.

The synthetic fraud definitions presented support the framework that SentiLink has shaped over the last several years. It is comprehensive, unambiguous, ties fraud to the perpetrator when appropriate, and helps identify the next best step in subsequent verification efforts. This framework also contemplates the following:

-
- ✓ The definition of First Party Fraud is confusing and can be interpreted both as (1) credit risk or (2) fraud risk. We believe that the current definition of First Party Fraud should not include consumer intent and instead should be defined purely on consumer identity and the potential tactics they may use to change identity attributes.
 - ✓ To clearly define synthetic fraud, we believe that the definition of Identity Theft should be altered to address the abuse of a third party's identity in whole or in part, in order to help distinguish between a fraudster's use of a consumer's identity and the consumer's misuse of their own identity.
 - ✓ Identity Mismatches occur and can show up as false positives in synthetic fraud models. We do not believe that consumer applicants identified as Identity Mismatches are synthetic fraudsters. However, we do believe they should have a place in the synthetic fraud definition discussion to help establish a common understanding around synthetic fraud false positives.
 - ✓ There are tactics used by consumers and fraudsters to build out and support both real and fake identities. While these tactics help enable fraud, there is some debate as to whether these tactics themselves are fraudulent, and we believe that stronger efforts should be taken to dissuade these activities.
-

The remainder of this white paper provides additional support and information related to the framework below.

SentiLink Synthetic Fraud Framework



Credit Risk

Consumer with no intent to pay using their real identity.
(is credit risk)



Fraud

First Party Fraud

occurs when a consumer applies for a loan using their real identity but has taken steps to manipulate *attributes* of their identity to obtain credit, with or without the intent to repay.

Synthetic Fraud

occurs when fraudsters combine fictitious and/or real information to create new identities with the intent of defrauding financial institutions, government entities and individuals.

Identity Theft

3rd party stolen identity that contains whole, or a *significant part*, of a consumer's identity.

First Party Synthetic

occurs when a consumer who has an SSN supplies their name, DOB, and a substantially different SSN than their own.

Third Party Synthetic

occurs when a fraudster who supplies a fictitious name, DOB, and SSN combination, where no combination of PII elements belong to any one real person.

Example Tactics

Boosted Trades

Paying non-reputable sources to report bolstered tradelines.

Credit Wash

Fraudulently cleaning legitimate negative tradelines from a credit report.

Piggybacking

Purchasing authorized tradelines from unknown sources.

False Documentation

Income, bank statements, etc.

Inquiries

Use loose CRA tradelines policies to create thin files.



Identity Mismatch

Data Quality (Consumer)

Pedantic: A consumer supplies their name, DOB, SSN but there is a typo in the SSN field.

Wrong DOBs: A consumer supplies their name and SSN but there is a typo in the DOB field.

Non-canonical: A consumer supplies their name, DOB, and SSN but the name they supply is a shortened version of their name.

Data Quality (Institutional)

Splinters: A consumer supplies their DOB and SSN, and the name they currently use, but incomplete information is retrieved due to split consumer records from name variants.

Other

Pre-SSN Issuance: A consumer supplies their name and DOB, but they have not been issued an SSN, so they supply a made up SSN.

A PROPOSED FRAMEWORK FOR DEFINING “SYNTHETIC FRAUD”

We propose that the industry adopt the Federal Reserve definition of “Synthetic Identity Fraud.” In order to provide more nuance, we also propose two sub-definitions to the Federal Reserve’s general definition. These two sub-definitions are based primarily on the entity that is perpetrating the fraud, and secondarily on the method by which the identity is created.

The Federal Reserve’s General Definition: Synthetic Identity Fraud

Synthetic Identity Fraud generally occurs when fraudsters combine fictitious and/or real information to create new identities with the intent of defrauding financial institutions, government entities, and individuals.

Sub-Definition 1: First Party Synthetic Fraud

First Party Synthetic Fraud occurs when a consumer who has an SSN supplies their name, DOB, and a substantially different SSN than their own.

First Party Synthetic Fraud is always perpetrated by the consumer who actually owns the identity provided during application. From our first-hand research across every industry, First Party Synthetic Fraud accounts for roughly 70% of all synthetic fraud and can generally be tied back to the real consumer. Tactics such as the illegal use of Credit Privacy Numbers (CPNs), “boosting tradelines,” “piggybacking,” and “credit washing” are deployed in sophisticated manners by first party synthetic fraudsters.



Sub-Definition 2: Third Party Synthetic Fraud

Third Party Synthetic Fraud occurs when a fraudster supplies a fictitious name, DOB, and SSN combination, where no combination of the PII elements belong to any one real person.

Third Party Synthetic Fraud is perpetrated by a third party who has completely made up an identity. While the identity may contain a real address or a valid SSN, the elements together do not belong to any real person. Third Party Synthetic Fraud accounts for roughly 30% of all synthetic fraud. Also referred to as “ghosts” or “Frankenstein” fraud, Third Party Synthetic Fraud is generally more organized and malicious in nature - and can consist of hundreds of fictitious identities deployed across sophisticated fraud rings in different geographic locations. However, it can also be perpetrated by a single person in a disorganized manner. Third Party Synthetics tend to use SSNs in the “random” range¹, boosted tradelines, “piggybacking,” and in some instances “credit washing” to help support their fictitious identities.

We strongly believe that a synthetic fraud framework that does not include a First Party Synthetic Fraud definition fails to address more than half of the synthetic fraud problem. A First Party Synthetic Fraud definition will help lenders optimize KYC and account opening verification procedures to better target the issue. While First Party Synthetic Fraud only results in financial loss about half of the time, it creates compliance issues 100% of the time for those industries who are required to follow KYC regulations.

Synthetic Fraud

occurs when fraudsters combine fictitious and/or real information to create new identities with the intent to defraud financial institutions, government entities, and individuals.

First Party Synthetic

occurs when a consumer who has an SSN supplies their name, DOB, and a substantially different SSN than their own.

Third Party Synthetic

occurs when a fraudster who supplies a fictitious name, DOB, and SSN combination, where no combination of PII elements belong to any one real person.

¹ Prior to 2011, SSN issuances were ordered such that state and time of issuance could be inferred. SSN issuances become completely randomized after 2011.



IDENTITY MISMATCHES BELONG IN THE SYNTHETIC FRAUD FRAMEWORK

From time to time, certain identities are classified as synthetic by machine learning models but, upon manual review, are actually “identity mismatches.” Identity mismatches are typically the results of typos, splintered files at the credit bureaus, or other data quality issues.

Identity mismatch issues do not typically result in financial loss. However they are pseudo-synthetic in nature and can create false positives in scoring models. Arguably, some identity mismatches may also create compliance risks for financial service companies and friction for consumers, especially when the SSN is substantially incorrect.




Fraud

Synthetic Fraud
occurs when fraudsters combine fictitious and/or real information to create new identities with the intent to defraud financial institutions, government entities, and individuals.

First Party Synthetic
occurs when a consumer who has an SSN supplies their name, DOB, and a substantially different SSN than their own.

Third Party Synthetic
occurs when a fraudster who supplies a fictitious name, DOB, and SSN combination, where no combination of PII elements belong to any one real person.



Identity Mismatch

Data Quality (Consumer)

- Pedantic:** A consumer supplies their name, DOB, SSN but there is a typo in the SSN field.
- Wrong DOBs:** A consumer supplies their name and SSN but there is a typo in the DOB field.
- Non-canonical:** A consumer supplies their name, DOB, and SSN but the name they supply is a shortened version of their name.

Data Quality (Institutional)

- Splinters:** A consumer supplies their DOB and SSN, and the name they currently use, but incomplete information is retrieved due to split consumer records from name variants.

Other

- Pre-SSN Issuance:** A consumer supplies their name and DOB, but they have not been issued an SSN, so they supply a made up SSN.

Within each of the identity mismatch categories, there are further sub-categories that include the following definitions:

Data Quality (Consumer)

Pedantic: A consumer supplies their name, DOB, and SSN but there is a typo in the SSN field.

Wrong DOB: A consumer supplies their name, DOB, and SSN but there is a typo in the DOB field.

Non-Canonical Identity: A consumer supplies their name, DOB, and SSN but the name they supply is a shortened version of their name.

Data Quality (Institutional)

Splinters: A consumer supplies their DOB and SSN and the name they currently use, but incomplete information is retrieved as a result of the existence of multiple consumer records from name variants.

Other

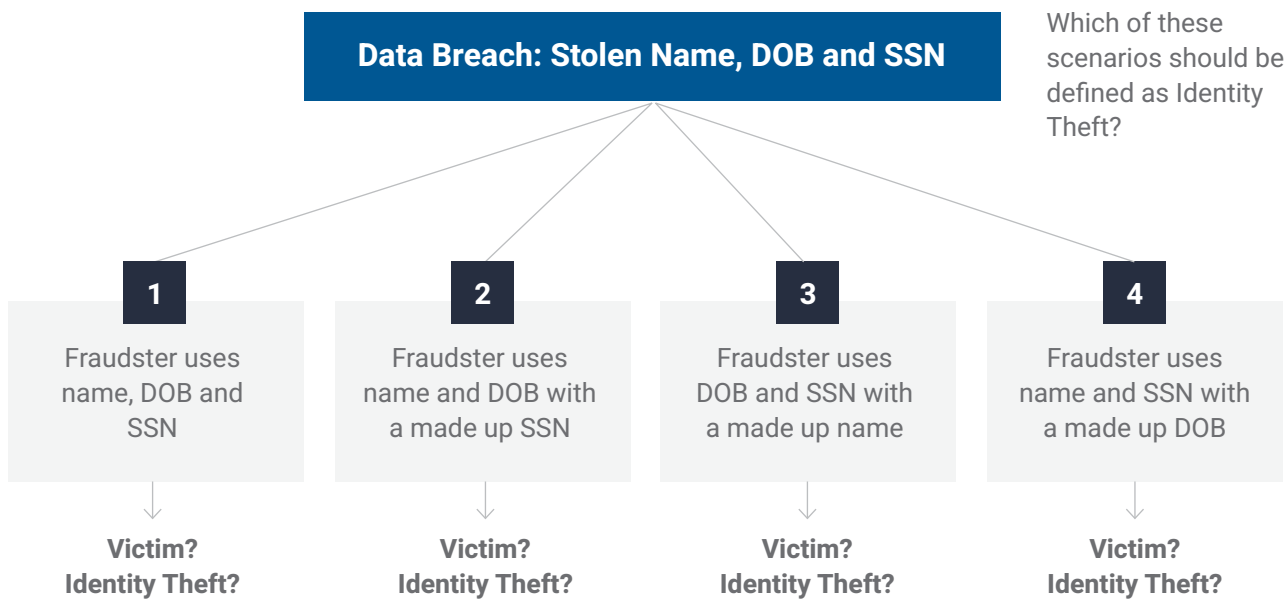
Pre-SSN Issuance: A consumer supplies their name and DOB, but they have not been issued an SSN so they supply a fake SSN. *It is important to note that a compliance driven organization may classify this behavior as first party synthetic fraud instead.*

If an institution properly identifies which type of non-malicious fraud behavior they are witnessing, they can properly address them with the correct verification strategy. For instance, if an application contains a wrong DOB, a reasonable course of action is to ask the consumer to re-enter their information.



AN UPDATED DEFINITION FOR IDENTITY THEFT

Consider a scenario in which a fraudster obtains data from a breach that exposed millions of consumer names, SSNs, and DOBs. The bad actor opens accounts fraudulently using a SSN and DOB combination that belongs to a real person along with a fake name, or a SSN and name combination belonging to a real consumer with a random DOB. Eventually, these opened accounts go unpaid and are reported as charge-offs to the credit reporting agencies.



In the scenarios illustrated above, could the fraudster's use of the stolen consumer identity result in consequences typically associated with identity theft, such as:

- Wrongful access of the consumer's credit report?
- The furnishing of misinformation to the consumer's credit report?

If the answer to with of those questions is "yes," then the definition of identity theft requires an update.

Today, identity theft is defined as “the fraudulent acquisition and use of a person’s private identifying information, usually for financial gain.” To ensure clarity and properly distinguish identity theft from synthetic fraud, we believe the definition for identity theft should be “the fraudulent acquisition and use of a person’s private identifying information by a third party, **in whole or a significant part**, usually for financial gain.”

The added language helps to distinguish between a person who is fraudulently manipulating their own identity (i.e., using a different SSN from the one they were issued) and a fraudster who has stolen a person’s identity and is using that identity, or some portion of it, for financial gain.

Our proposed modification to the current definition of identity theft expands its applicability beyond scenario 1 to scenarios 3 and 4.

Fraud

Synthetic Fraud
occurs when fraudsters combine fictitious and/or real information to create new identities with the intent to defraud financial institutions, government entities, and individuals.

Identity Theft
3rd party stolen identity that contains whole, or a significant part, of a consumer’s identity.

First Party Synthetic
occurs when a consumer who has an SSN supplies their name, DOB, and a substantially different SSN than their own.

Third Party Synthetic
occurs when a fraudster who supplies a fictitious name, DOB, and SSN combination, where no combination of PII elements belong to any one real person.

We believe these instances of identity manipulation would likely impact the consumer’s credit report directly, thereby creating a clear and real victim.



DEFINING FIRST PARTY FRAUD WILL HELP CREATE CLARITY FOR SYNTHETIC DEFINITIONS

First Party Fraud has differing definitions depending upon who or what company you ask. For example:

“We call this a hybrid form of risk because **it includes elements of both credit and fraud risk**. Specifically, first party fraud involves an individual who makes a promise of future repayment in exchange for goods / services without the intent to repay.”

Experian

First party fraud, also known as credit muling, typically occurs when an individual obtains a loan with no intention of repayment. This can also occur by **defaulting a depository account** without repayment”.

TransUnion

“Often referred to as “**credit muling**” or “**equipment gaming**,” first-party fraud occurs when consumers use their true identities and personal information to apply for multiple, high-value products with no intention of honoring their contractual agreements.”

ID Analytics

“First party fraud is where an individual, or group of people, **misrepresent their identity or give false information**. This is usually done when applying for a product or service to receive more favourable rates, or if they have no intention of meeting their commitments. Another example could be if an individual can make a false claim against an insurer to obtain a payment they are not eligible for.”

Experian

“First Party Fraud is so-named because it involves a bad actor essentially representing themselves AS themselves – in the first-person, as it were. As with the other types of fraud we’re discussing, misrepresentation is still the key to the attack, but in the case of First Party Fraud, the fraudster is not misrepresenting who they are, but rather, **they’re being deceptive about their information**, and their intentions.”

Datavisor

While there is not a generally accepted definition of first party fraud, at its simplest, it could be defined as “a consumer who applies for a loan using their real identity with no intent to repay.” In this form, the definition of first party fraud sounds more like credit risk though further specification reveals that the issue is actually a fraud problem.

There are two options to clarify the definition of first party fraud:

1. Leave the definition “as is” but clearly define it as credit risk.
2. Expand the current definition of first party fraud to address the fraud characteristics involved such that the meaning of first party fraud reflects a fraud definition (attributes refer to credit washing, piggybacking, boosted tradelines, etc.).

Based on the behaviors observed with respect to first party fraud, we propose expanding the definition to address the fraud characteristics involved.

Proposed First Party Fraud Definition

First Party Fraud refers to a consumer that applies for a loan using their real identity but has taken steps to manipulate **attributes** of their identity to obtain credit, with or without the intent to repay.

Therefore, first party fraud would clearly fall in the fraud space while acknowledging the person committing the fraud is using identity information that belongs to them, which creates differentiation from the synthetic fraud definitions.

The addition of “with or without the intent to pay” helps us capture those consumers who may actually have the intent to repay, but are actively manipulating their identity attributes in order to obtain credit or gain credit at better terms.





Credit Risk

Consumer with no intent to pay using their real identity.
(is credit risk)



Fraud

First Party Fraud

occurs when a consumer applies for a loan using their real identity but has taken steps to manipulate attributes of their identity to obtain credit, with or without the intent to repay.

Synthetic Fraud

occurs when fraudsters combine fictitious and/or real information to create new identities with the intent to defraud financial institutions, government entities, and individuals.

Identity Theft

3rd party stolen identity that contains whole, or a significant part, of a consumer's identity.

First Party Synthetic

occurs when a consumer who has an SSN supplies their name, DOB, and a substantially different SSN than their own.

Third Party Synthetic

occurs when a fraudster who supplies a fictitious name, DOB, and SSN combination, where no combination of PII elements belong to any one real person.

Example Tactics

Boosted Trades

Paying non-reputable sources to report bolstered tradelines.

Credit Wash

Fraudulently cleaning legitimate negative tradelines from a credit report.

Piggybacking

Purchasing authorized tradelines from unknown sources.

False Documentation

Income, bank statements, etc.

Inquiries

Use loose CRA tradelines policies to create thin files.

The "attributes" that are being changed by consumers also need to be defined. Additionally, there needs to be clear regulatory and legal interpretations of these behaviors as fraudulent. An entire industry has been created to help Americans repair and enhance their credit score. Many U.S. consumers have used these companies to legitimately raise their scores. However, a handful of non-reputable credit repair agencies with limited identity verification controls are regularly abused by synthetic fraudsters looking to build credit histories quickly.

Here are examples of tactics that change identity attributes:

Credit Washing

After a legitimate consumer has maxed out credit and potentially missed payments, they falsely claim to be the victim of identity theft through the credit report request and undergo the dispute and investigation processes at either a credit reporting agency or the lender. This often results in legitimately reported tradelines being removed from the consumer's credit report, otherwise known as "credit washing." As a result, financial institutions who subsequently pull credit on this consumer may not see large derogatory lines of credit which were maxed out and closed for non-payment.

Both real consumers and synthetic fraudsters commit credit washing. Our analysis shows that credit washing is performed in 11% of first party synthetic cases and 13% of third party synthetic cases. We did not analyze first party fraud in our study.

Boosted Tradelines

There are a number of credit repair companies and lenders offering products that overstate the credit relationship a consumer may have with them. These credit products look like legitimate tradelines and can falsely drive down utilization rates.

SentiLink analyzed 10 credit reports that each had a \$5,000 tradeline from one of these types of companies. 7 of the 10 reports analyzed listed the lender tradeline as the first tradeline opened by the fraudster. In all 10 credit reports, there was a zero balance on the non-reputable lender tradeline, which likely signifies that the fraudsters had no intention of using the credit issued. It also indicates that the non-reputable lender bears little to no risk in approving these unsecured loans for fraudsters since they aren't used for credit, but rather, to improve credit utilization.

Piggybacking

Many first party and synthetic fraud identities purchase authorized user tradelines, a practice known as "piggybacking," from sites online that sell access to others' tradelines. Legitimate consumers can also purchase tradelines from these websites. In the situation where a legitimate consumer "piggybacks" on a purchased authorized user tradeline, the consumer should be classified as a first party fraud because the consumer is fraudulently bolstering their credit score. This tactic is technically not illegal, although most lender agreements for credit vehicles that have authorized users point this out as breach of contract.

Document Fraud

Document fraud is the manufacturing, counterfeiting, alteration, sale, and/or use of identity documents and other fraudulent documents for criminal activity, including financial fraud. Legitimate consumers and fraudsters alter bank statements, tax forms, and other documentation to gain credit at better terms.

IN SUMMARY

Since its inception, SentiLink has been laser-focused on the problem of synthetic fraud. Our data scientists have analyzed billions of consumer records, our products have scored millions of applications, and our fraud analysts have manually labeled over 100,000 synthetic fraud cases. The synthetic fraud framework outlined in this white paper has been developed to address the various behaviors we observe and has been honed over years of experience. It is comprehensive, unambiguous, ties fraud to the perpetrator when appropriate, and helps identify the next best step in subsequent verification efforts.

We support industry and government efforts to establish more solid definitions surrounding synthetic fraud and offer up our learnings to help fuel discussion.

As groups debate synthetic fraud, we hope the following issues will be addressed:

- ✓ **Clarifying any confusion around the existing definition of first party fraud, which creates complications for data sharing, treatment strategies, and regulatory governance.**
- ✓ **Broadening the definition of identity theft to include “in whole or in part” in order to address identity theft-related consequences.**
- ✓ **Establishing sub-definitions for synthetic fraud that inform and optimize verification methods and reduce consumer friction in application processes.**
- ✓ **Recognizing first party fraud as an identity manipulation and fraud problem and establishing regulatory guidance to help lenders identify and take recourse against these tactics when abused.**

We are excited to play a part in establishing common definitions.



ADDITIONAL RESOURCES

General Synthetic Fraud Discussion

[Federal Reserve, Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors, July 2019](#)

[Federal Reserve, Payments Fraud Insights, Detecting Synthetic Identity Fraud in the U.S. Payment System, October 2019](#)

[Federal Reserve, Payments Fraud Insights, Mitigating Synthetic Identity Fraud in the U.S. Payment System, July 2020](#)

[Equifax, Synthetic Fraud: A Look Behind the Mask, 2019](#)

[Experian, Synthetic Identities: Getting real with customers, 2017](#)

Giact, The Hidden Costs of Synthetic Fraud, 2019

[ID Analytics, The Long Con: An Analysis of Synthetic Identities, October 2014](#)

IDology, Fighting Back with Multi-Layered Solutions

[McKinsey, Fighting back against synthetic identity fraud, January 2019](#)

[Mitek Systems, Fraud Trends and Tectonics, 2020](#)

[TransUnion: Synthetic Identity Fraud, 2020](#)

[Verafin, Synthetic Identity Fraud, Infographic](#)

Synthetic Fraud Tactics

[The Better Identity Coalition: A Blueprint for Policy Makers, July 2018](#)

[Federal Trade Commission, FTC says credit repair company en-CROA-ched on consumer rights, June 2019](#)

SSN Randomization

[Alessandro Acquisti and Ralph Gross, Predicting Social Security numbers from public data, July 2009](#)

[ID Analytics, Exploring the Impact of SSN Randomization, March 2015](#)