Identity and fraud trends report

Q2 2021: **Synthetic identity fraud**

While many businesses spent 2020 "heads down" navigating unexpected detours associated with the COVID-19 global pandemic, enterprising criminals sprang into action.

New fraud types roared onto the scene, with the Federal Trade Commission fielding more than 325,000 pandemic-related reports of fraud and identity theft from January 2020 through April 2021.[1] At the same time, existing fraud types — think: synthetic identity fraud, authorized user abuse and credit piggybacking — are rising, according to internal studies by Equifax. Here, we share the results of those analyses.

Introducing: **The Identity and fraud trends report from Equifax.**

This new quarterly report will help organizations better protect against fraud threats by exposing the top trends we're seeing in the market.

Knowing that you can't battle what you can't see, our goal is simple. We're providing timely, hyper-relevant insights to help businesses better understand new and existing fraud schemes. Packed with data, trends and "pro tips" from our expert team of fraud analysts, the report offers a big-picture fraud perspective and a rare opportunity for companies to benchmark fraud activity with their portfolios.

Each quarterly report will have a dedicated fraud focus, with this report focusing on synthetic identity fraud. Inside, you'll read about year-over-year synthetic ID trends and get first-hand "insider" information and insights on fraud mitigation best practices.

You'll get fresh ideas for intelligently differentiating and detecting suspicious activity. That way, you can put guard rails around it and steer legitimate, qualified customers toward a path of financial empowerment.

Fraud is escalating. It's time to act. Keep reading for actionable data and insights to help you better detect and fight fraud across your organization, at every step of the customer journey.

Sid Singh, *USIS President, Equifax*

"As the coronavirus vaccine has become more readily available in the U.S., the signs of economic recovery are all around us.
We are ready to help our customers look ahead to the post-pandemic future.
That future is one where fraud detection and prevention are becoming an increasing priority for businesses large and small...
[it is] more important than ever that our customers invest in people, processes and technology to fight fraudsters."

Synthetic identity fraud:
A foundational fraud scheme.

Unlike traditional identity theft, where a consumer's personally identifiable information (PII) is stolen and used to obtain financial products, synthetic identities are fictional. They can include a hodge-podge of real information — bits and pieces of real names, addresses and SSNs from different people — or a combination of real and fake information.

Once the identity is created, criminals start building a credit history associated with the identity, often by first becoming an authorized user of someone else's good account. They then start applying for credit. This legitimizes the synthetic identity's credit and as a result the identities look like real people and creditworthy consumers, which is what makes synthetic identities hard to detect.

While synthetic identity fraud is a global fraud issue, it's important to note that it's also the foundation of other fraud schemes like authorized user abuse and credit piggybacking. Put simply, the issues aren't separate; instead, they're intertwined.

- **Authorized user abuse.** The synthetic identity fraudster may pay a primary account holder to allow them to become an authorized user on their good account. This is collusion where both parties benefit. This relationship gives the authorized user direct access to the primary user's credit line and accompanying history.
- **Authorized user velocity risk.** A notable risk of authorized use abuse is when organized crime rings continually add synthetic identities to credit cards as authorized users over time. We call this authorized user velocity risk.
- **Credit piggybacking.** Authorized user abuse is a form of credit piggybacking, in which fraudsters use information from legitimate card holders who are in good standing. This can manifest into credit boosting schemes tied to credit repair and other fraud types. While not all piggybacking is fraud, it can point to an increased potential for fraud as criminals look for ways to activate synthetic identities.

3:1

One out of every three false positives we see is actually a synthetic identity.

One portfolio. **$25 million in fraud charge-offs.**

A recent portfolio-specific Equifax study redlined $25 million in potential charge-offs in one year due to fraud charges associated with authorized user abuse. Within that same portfolio, more than 62,000 existing accounts were identified as potential synthetic identities, which could easily result in **$8 million+ losses in a single year**.

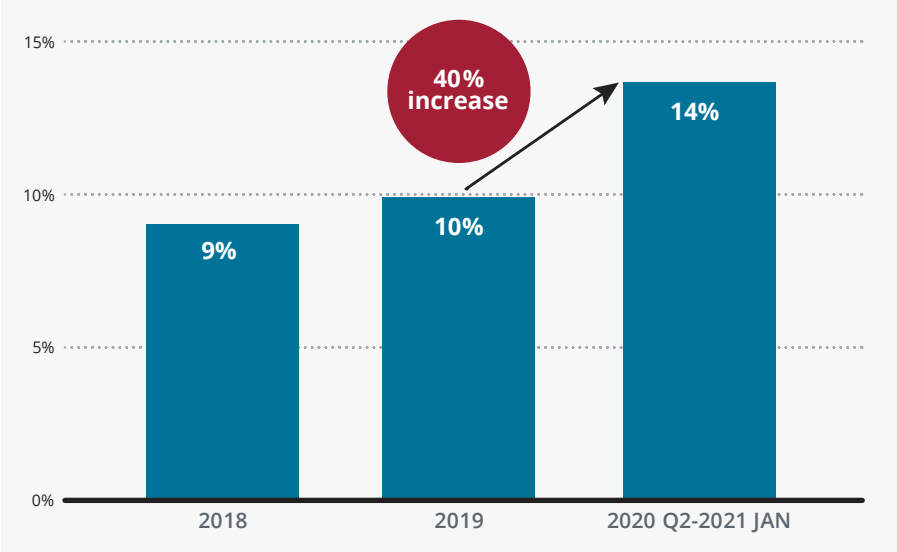
— Equifax Case Study, ***Tackling fraud initiated through authorized user abuse***

Synthetic identity fraud and consumer credit.

To explore the synthetic identity risk trend related to authorized user abuse, we monitor consumer activities based on inquiry transactions. Our data and insights around synthetic identity reveal a shift fueled by the accelerated move toward "faceless," online channels during 2020. As a result, we're seeing double-digit increases across specific fraud types.

After the Covid19 outbreak in April 2020, we saw that fraudsters were more likely to use credit piggybacking. Figure 1 shows credit piggybacking usage among suspicious synthetic identities increased by 40 percent through January 2021.

Figure 1: Credit piggybacking among suspicious synthetic identities



Synthetic identity

It's all about control.

Equifax-captured synthetic identities reveal that accounts are typically created with a **postal address**, **phone number** and **email address** that the fraudster can control.

A recent Equifax study identified roughly

1.8 million

consumer credit accounts as potential **synthetic identity fraud** within the time span of one year.

More than

30%

of these accounts were at risk of major delinquency or **charge-offs** with **average losses** of

$8,000-$10,000

per case.

— Internal Equifax findings

In Figures 2 and 3, we see authorized user velocity risk has slowly but steadily increased from January 2018 through January 2021 by 26 percent.

Figure 2: Authorized user abuse velocity risk: Quarterly analysis

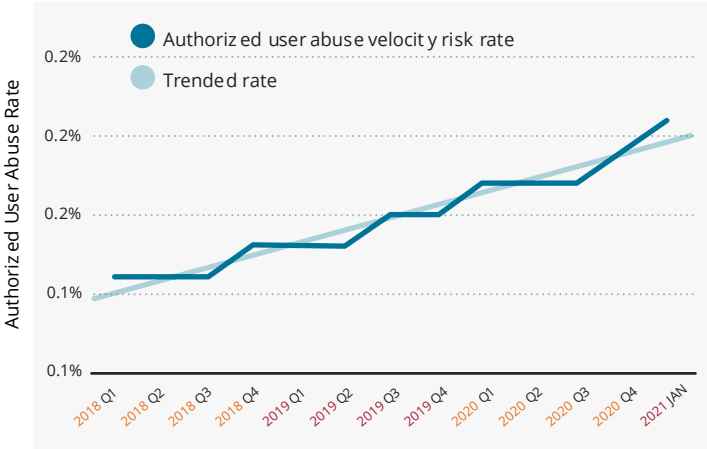
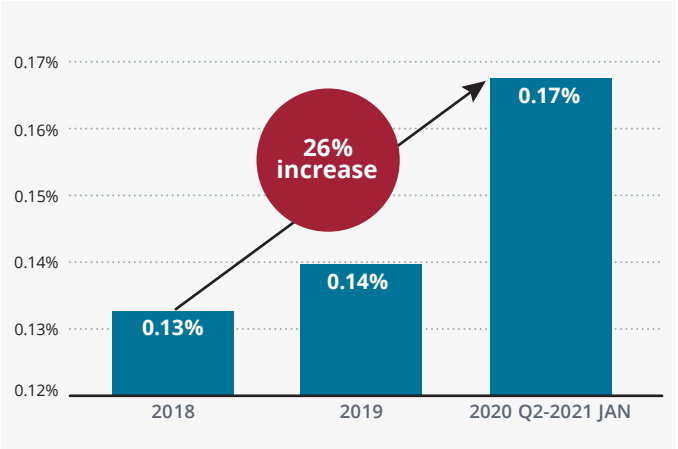
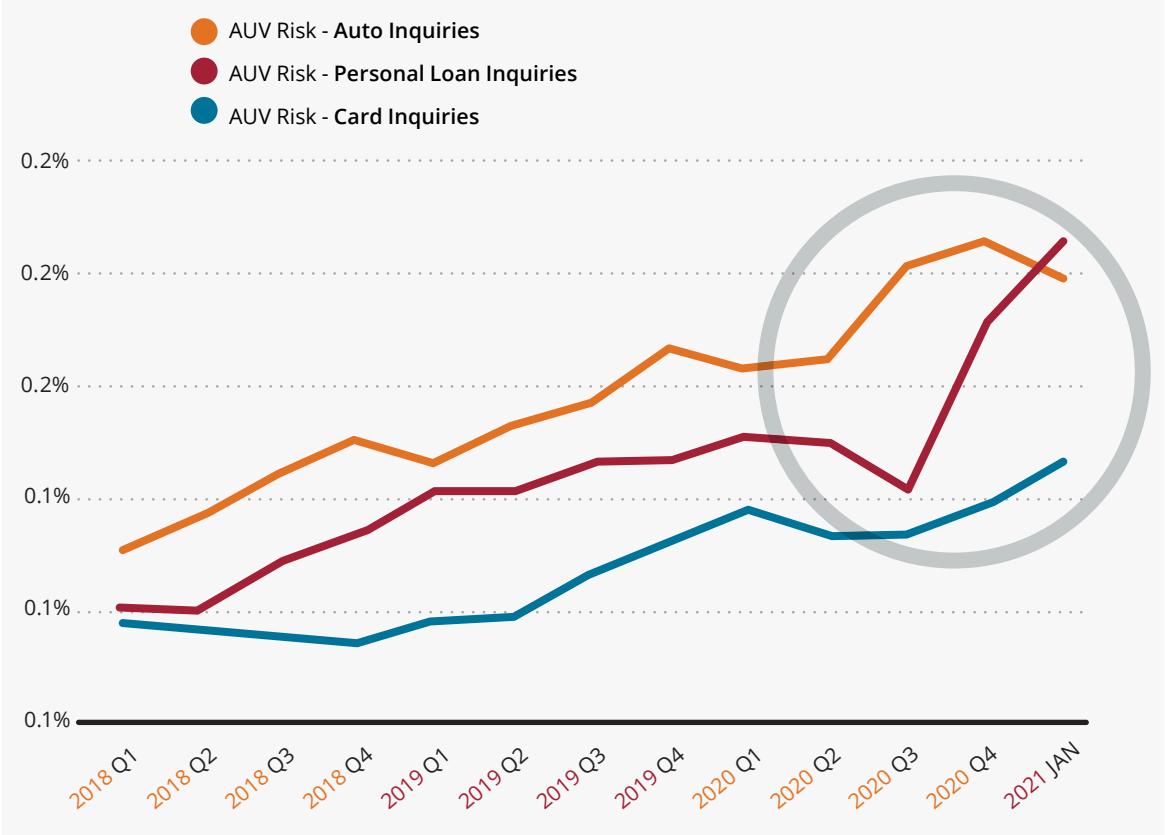


Figure 3: Authorized user abuse velocity risk: Year over year analysis



Interestingly, in Figure 4, we see authorized user velocity (AUV) risk is an increasing trend seen across all different lending portfolios: card, auto loans and personal loans.

Figure 4: Authorized user abuse, velocity risk: Lending portfolio analysis

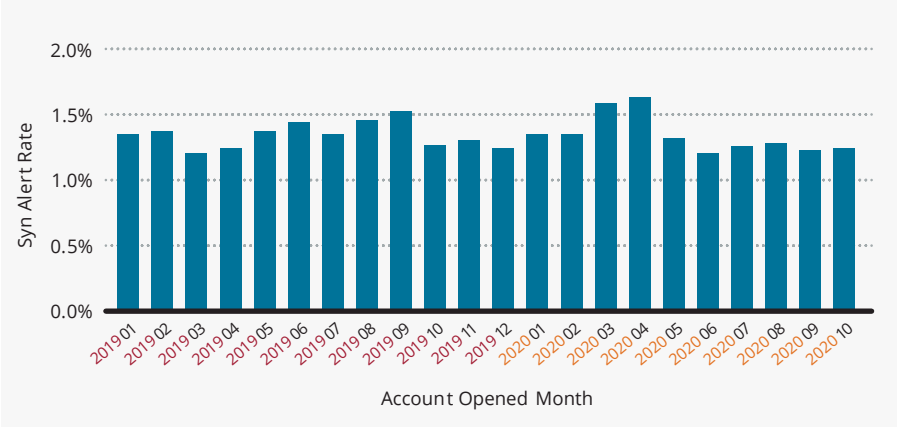


To track the impact of synthetic identity fraud risk for credit and lending industries, we monitor two trends:

- the synthetic identity alert rate (which represents the potential synthetic identity risk on the booked portfolio) shown on booked accounts.
- the booked accounts performance (e.g. delinquency) based on the trades reported to the Equifax consumer credit file.

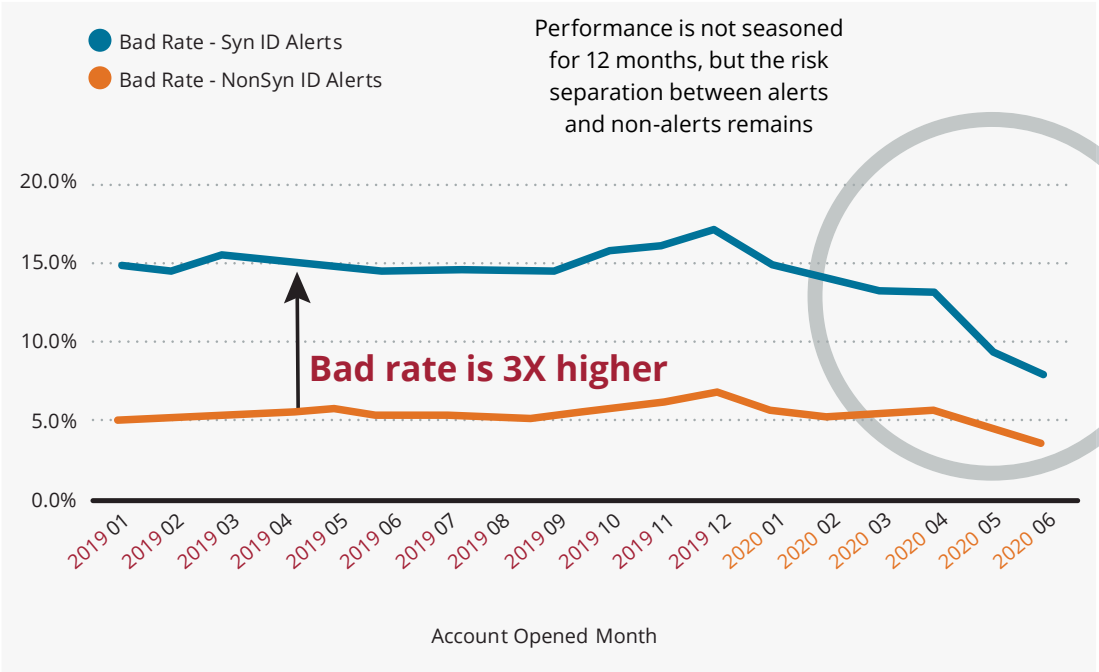
As we see in Figure 5, synthetic identity alert rates were high in 2020 March and April, but after 2020 April the alert rate returned to the normal level around 1.3 percent.

Figure 5: Synthetic identity fraud risk on the booked accounts



In Figure 6, we see stark differences in bad rates. "Bad" accounts are 60 days past due (DPD) or worse in 12 months on the book. The bad rate among the synthetic identity alerts remained stable over time, yet it is three times higher than the non-synthetic identity alerts.

Figure 6: Bad rate (60 DPD+ in 12 MoB) — Performance observed 2020 Dec



Behind the numbers.

As criminals focused their efforts on the "opportunity of the moment," namely government benefit and stimulus payments, synthetic fraud activity slowed during 2020.

However, given the year-over-year increases in credit piggybacking and authorized user velocity risk from 2018 to 2021, it's clear that a lack of comprehensive synthetic identity fraud control remains an industry issue. In a post-pandemic era, reducing synthetic identity risk on the books is a top priority for fraud executives.

What's more, the surge in use of online services last year increased the potential for fraud, prompting businesses such as auto dealers, banks, credit unions and online lenders that use digital services to focus on strengthening user identity verification and authentication. Recognizing their increased vulnerability to identity verification risks, businesses are taking action.

In a recent survey conducted by Equifax and PYMNTS.COM, almost half of the participants plan to invest in digital ID solutions to address these concerns.

Equifax/PYMNTS.com survey, July 2021

Top reasons to invest in digital ID solutions:

Increase the number of customers
68.4%

Improve the number of completed customer transactions
68.1%

Streamline disparate systems into a single process or system
63.2%

Increase levels of trust among customers
67.4%

Four keys to fighting identity fraud

DATA

Supplement internal anti-fraud tools with multi-dimensional data resources from credit reporting agencies and data aggregators specializing in fraud. This information uncovers "proof of life" behavior characteristics of legitimate applicants.

BEST PRACTICES

Use fast, reliable identity verification techniques that check applications against multiple sets of public and proprietary data to confirm things like:

- Is the address real?
- Is there an employment record or a registered vehicle?
- Are there utility accounts?

TECHNOLOGY

Use machine learning algorithms to help discover identity discrepancies and unique behavior patterns, such as authorized user abuse, that may transcend multiple accounts at multiple creditors. This can help increase detection rates while lowering false positives — in essence, providing a better experience for the consumer.

ANALYTICS

Use data analytics to detect linkages and suspicious patterns indicative of phony or manipulated identities. For example, by comparing a SSN to a consumer's PII, algorithms can determine how well a supplied SSN matches its identity. A positive SSN confirmation along with several negative alerts can signal the creation of a synthetic identity or other SSN-related fraud account opening.

Fighting synthetic identity fraud:
A layered approach.

Fighting synthetic identity fraud isn't easy. It's a constant battle to keep up with high-tech, fast-moving fraudsters. Due to the inherent complexities associated with this type of fraud, a layered approach is best.

Relying on an outdated fraud mitigation strategy or legacy technology system isn't enough to stay ahead of today's sophisticated criminals. You must continually evolve and manage your mitigation processes and strategies across all channels. That means layering your defenses the same way you would protect your home.

Think of it this way. If you're securing your home, you lock the front door, but you don't stop there. You also lock the back door and all your windows. As technology advances, you add a camera to your doorbell, maybe a wireless alarm system and, eventually, you can control everything from your smartphone. The same is true when it comes to protecting your business.

"Think of it this way. If you're securing your home, you lock the front door, but you don't stop there. You also lock the back door and all your windows. As technology advances, you add a camera to your doorbell, maybe a wireless alarm system and, eventually, you can control everything from your smartphone.

The same is true when it comes to protecting your business."

Here's an example of how we worked with a customer to develop a layered approach that effectively combats fraudulent online card applications.

Challenge

A top bank identified significant fraud from card accounts initiated online, resulting in notable write-offs and administrative follow up.

Solution

Implement a three-pronged approach to identify online card accounts within its portfolio that may have been created with synthetic identities.

The bank's layered approach included:

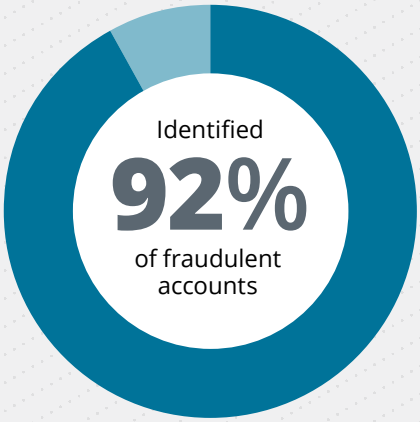
Integrate alerts triggered by machine learning algorithms that use multidata sources to detect synthetic IDs and patterns.

Automatically assess the validity of account holders' emails in real time.

Automatically confirm account holders' phone numbers via data match in real time.

Result

The combined solutions captured 92 percent of fraudulent accounts.



Pro tips to advance your program

1 Identify synthetic identity fraud that might be hiding in credit losses.

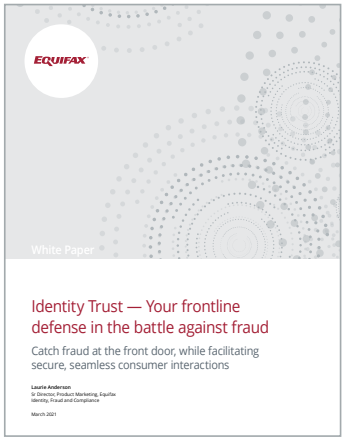
Synthetic identities are hard to detect, often miscategorized as never pays, write offs, bad debts or other credit losses. Businesses get tripped up on this and focus on the fraud write-offs instead of heading fraud off at the pass and avoiding the losses altogether. Having a thorough taxonomy between credit risk and fraud risk allows businesses to measure risks more accurately.

Read this blog article to learn the latest identity verification techniques:

- **Identify and weed out fraud.**
- **Allow good risk in and keep poor risk at bay.**
- **Mitigate fraud losses.**
- **Properly classify losses.**

2 Bridge the trust gap early and often.

Fraudsters often open Demand Deposit Accounts (DDAs) to create foot-in-the-door access to other lines of credit. Once the red carpet is rolled out for the “new” or “existing” customer, the fraudster is offered other products, like credit cards and loans. This is where the real losses occur. Bridging the trust gap early and often between customers and businesses is critical to identifying synthetic identity fraud before the losses start soaring. This involves working behind the scenes to verify the identity and intent behind every digital, “faceless” transaction.



Read this white paper to learn how establishing identity trust plays an essential role in the fight against fraud.

- **Trust consumer identities in real time across any digital interaction.**
- **Strengthen and protect the entire customer journey.**
- **Increase approval rates and revenue.**
- **Reduce manual reviews, false positives and chargebacks.**

Analyst insights

As part of our identity and fraud risk "dream team," Cori Shen knows a lot about synthetic identity fraud. Here, she shares her insider knowledge and tips to help businesses better detect and stop the spread of this hard-to-spot fraud.

Q: What should businesses be looking for related to synthetic identities?

A: Search for abnormal signals throughout the identity's lifecycle, including applying for loans or cards, making payments on accounts, checking credit scores online and even updating account information.

- When fraudsters create synthetic identities, they could wait years before they make a move. But, once they do, it's extreme. They frantically shop for money from multiple banks, credit card providers and other lenders — all at the same time. They also anxiously check their credit, almost on a daily basis.
- Synthetic identities can appear as outliers at an early stage. Some will immediately apply for high-dollar loans like luxury vehicles from the start. Normal consumer identities start small as they try to slowly build their credit.
- And last, they frequently change their account information — things like address, phone and email — from various digital devices.

This is why it's important to assemble a connected, actionable view of credit and identity data across the organization, one that's enriched with multisource data. When it's done right, this "smart data" can talk and show you high-risk anomalies that you would otherwise overlook.

Q: Can you provide a specific example of how "smart data" can help?

A: Here's a great example. It is standard that with good digital identity tools we can quickly identify the abnormal digital signals (like IP, geo-location outlier, proxy risk, etc.) when fraudsters use a tablet or smartphone to update their account information.

Yet, we can also see authorized user abuse risks associated with "identities." Smart data can assemble all types of data insights from several sources to harness the power of connected insights, so you can take actions. Many times, these insights connect with three or four degrees of separation, but a graph network connection can bring them together. To hear more about our Smart Data approach, **click here**.

Q: Once a synthetic identity is "approved" as a customer, how long before the fraudster uses that account to commit fraud?

A: Interestingly, the sudden "activation" of synthetic identities happens at a somewhat predictable pace, based on credit type and industry.

- Personal loans often go bad in the first six months.
- About 50 percent of credit cards tend to go bad right away within the first six to eight months, while the rest can take up to 18 months to go bad.
- Auto loans gradually go bad between four months and 24 months.

Q: Are there any emerging trends you're seeing in your research?

A: Yes. We know that authorized user abuse is a form of credit manipulation used by fraudsters to bolster the credit for their synthetic identities, but we are spotting more malicious credit manipulation patterns such as credit washing. Credit washing occurs when a consumer disputes one or more legitimate items included in their tradeline history, claiming they were a victim of identity theft. The goal is to "wash" the negative information from their credit report and boost their credit score.

Cori Shen, *Equifax Data Science and Analytics Director*

We've seen credit washing increase since 2018 and believe that it and other similar fraud types are the emerging "authorized user abuse." This poses a risk to the larger credit market, in that it can:

- Enable fraudsters to steal millions of dollars from financial institutions.
- Prevent legitimate, creditworthy consumers from accessing credit, since financial firms will likely respond by tightening their risk policies.
- Increase synthetic identities fraud rates, as synthetic identities are likely to use this scheme. And synthetic identity risk not only impacts the consumer lending industry. With the advent of the Paycheck Protection Program (PPP), government and commercial entities are also having to address manipulated or fabricated identities used to secure loans under false pretenses.
- Further increase fraud losses since this type of activity can occur repeatedly over the lifetime of the identity.

Learn More

SIGN ME UP

Get the next Identity and fraud trends report — hot off the presses — in your inbox, as soon as it's available!

LISTEN NOW

Access our Data Dialogues podcast about using "smart data" to combat Identity fraud.

EQUIFAX INSIGHTS

Get the latest fraud insights, including quarterly analyses of the Equifax consumer credit file on our **blog**.

LINKEDIN

See what top fraud experts are talking about! Follow Equifax and our rock-star analytics team on LinkedIn.

Sriram Tirunellayi, Equifax VP of Data & Analytics

Cori Shen, Equifax Data Science & Analytics Director

equifax.com/business • 404.885.8500 • equifax.com/business/prevent-fraud/

[1] https://public.tableau.com/profile/federal.trade.commission?utm_source=govdelivery#!/vizhome/COVID-19andStimulusReports/Map