



EQUIFAX®

The Future of Fraud



PART I

What businesses need to know about
identity fraud, post pandemic.

2021



The opinions, estimates and forecasts presented herein are for general information use only. This material is based upon information that we consider to be reliable, but we do not represent that it is accurate or complete. No person should consider distribution of this material as making any representation or warranty with respect to such material and should not rely upon it as such. Equifax does not assume any liability for any loss that may result from the reliance by any person upon any such information or opinions. Such information and opinions are subject to change without notice. The opinions, estimates, forecasts, and other views published herein by the Equifax Economic Insights group represent the views of that presenter group as of the date indicated and do not necessarily represent the views of Equifax or its management.

Wherever there are businesses and consumers with money, there are fraudsters attempting to take it.

Fraud is complicated. It can happen anywhere, anytime, across virtually any channel, to any business or consumer. Analysts and experts who study fraud understand its' pervasive, shape-shifting nature. They know fraudsters go after two things: money and vulnerability.

The COVID-19 global pandemic is a painful example. More than \$397 million was lost to pandemic-related schemes and fraud as of early April 2021, according to the Federal Trade Commission.¹ As unprecedented volumes of activity and transactions shifted online during ongoing lockdowns, losses due to identity theft — the foundation of other schemes like application fraud, account takeover fraud and more — surged 42 percent from 2019 to 2020, according to a report by Aite Group.²

Moving forward, fraudsters will continue to follow the money trail, attack vulnerable touchpoints and transactions and wreak financial havoc on businesses that are largely unprepared.

Fraudsters go after two things: money and vulnerability.



Losses due to identity theft are projected to hit \$721.3B in 2021

Aite – The Stark Reality of Fraud (2021)

It's time to wake up.

Right now, it is too easy for criminals to commit fraud, according to a 2020 Javelin fraud study.³ It's not a matter of *if*, but *when* and *how much* fraud will impact your business.

- By 2023, losses from identity theft are estimated to reach \$635.4 billion.²
- Up to 13 percent of consumers are unlikely to use a financial institution where a fraudulent account was opened in their name.²
- Fraudulent synthetic identity accounts that go undetected on the books for 24 months drive estimated total losses of \$200 million per month — \$2 billion annually — according to a 2021 analysis of the Equifax consumer credit file.
- This ebook examines a few of the latest fraud trends, offering context and insight around their trajectory and impact on businesses. Then, it zooms out to discuss how and where these criminal schemes impact the customer journey, at a pivotal time when “improving the customer experience” is increasingly factored into fraud investments.

This ebook examines a few of the latest fraud trends, offering context and insight around their trajectory and impact on businesses. Then, it zooms out to discuss how and where these criminal schemes impact the customer journey, at a pivotal time when “improving the customer experience” is increasingly factored into fraud investments. Last, it explores advanced data strategies, technologies and AI-fueled modeling techniques available to help businesses mitigate fraud risk *and* support business growth. You'll get the information, insights and ideas you need to take action today, so you'll be ready and waiting to check criminals at the front door.



Where traditional approaches are fueled by siloed data and technologies, next-gen identity and fraud solutions are powered by data, attributes advanced modeling techniques and even platforms — all across a single enterprise.

Sriram Tirunellayi

VP of Data and Analytics
Equifax

A photograph of two men in an office setting at night. The man on the left, wearing glasses and a dark sweater, is pointing at a computer monitor. The man on the right, wearing a denim shirt, is looking at the screen. The background is dark with some blurred lights.

**What's driving
fraud losses?**
These trends.

Buy Now Pay Later

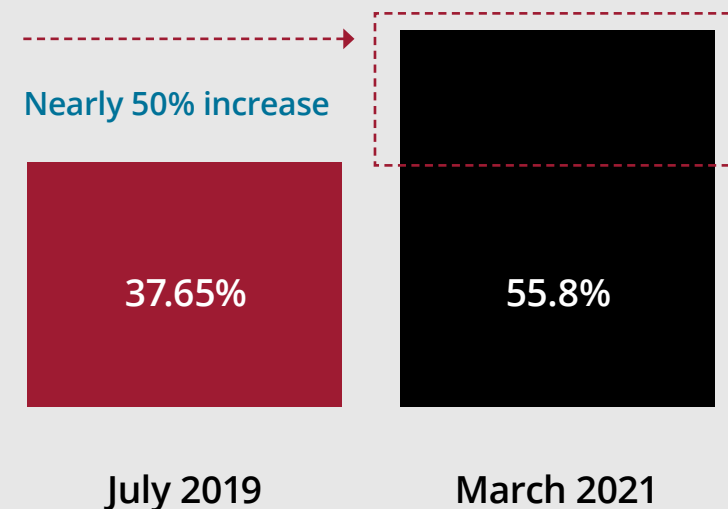
In less than a year, the number of consumers using buy now pay later (BNPL) services soared nearly 50 percent, up from 37 percent in July, 2020, to nearly 56 percent in March of 2021.⁵ Also known as “point of sale credit,” it’s exactly what it says: consumers can buy now and pay later in a series of installments over a pre-set time frame. By 2025, the industry is on track to hit a global transaction volume of \$680 billion.⁶

Trust and transaction volumes are driving fraud in this industry. BNPL providers sometimes perform “soft” identity and credit inquiries on consumers at the point of sale. This involves largely trusting the consumer can and will make their payments after receiving the product. In turn, the sheer ease of the transaction — combined with pandemic-driven shifts to online purchases — have fueled increased transaction volumes.

Fraudsters see these “low-barrier,” high-volume transactions as opportunities to:

1. Steal consumer information;
2. Use fake identities or “mule” identities with less chance of getting caught;
3. Obtain a BNPL loan or credit line with no intent to pay; and
4. “Loan stack,” which involves taking out multiple loans or lines of credit within a very short period of time, often 36-48 hours, with no intention of paying.

Consumers use of Buy Now Pay Later Services



<https://fool.com/the-ascent/research/buy-now-pay-later-statistics>

In less than a year, the number of consumers using buy now pay later (BNPL) services soared nearly 50 percent.



\$2.42
billion

A **conservative** estimate
of synthetic identity
fraud losses by 2023.

Aite Group

Synthetic Identity

Unlike identity theft fraud where a criminal steals an individual's personally identifying information and uses it to commit fraud, synthetic identities are completely made up. These fake identities, which may or may not include bit and pieces of real identities, are then used to open fraudulent accounts, credit lines and more. Up to 70 percent of fraud executives participating in a recent Aite Group study believe synthetic identity fraud is a bigger challenge than identity theft.⁸

Why? Synthetic identities look and feel like real people and they're often used via online "faceless" channels, all which makes it difficult to detect.

Equifax data supports the growing concern. As part of an ongoing analysis of our consumer credit file, we find the bad rate — when fraudulent activity is suspected — among accounts with synthetic identity alerts is **three times** higher than bad rates associated with non-synthetic identity alerts.

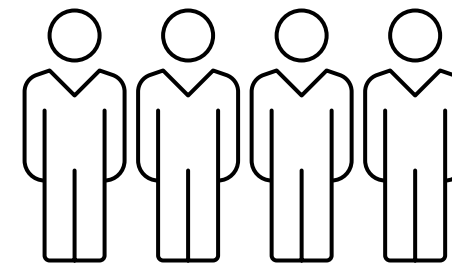
Further, we see the synthetic identity rate is particularly high among accounts opened after 2020 April, pointing to an increased synthetic identity risk after the COVID-19 outbreak.

Up to 70 percent of fraud executives participating in a recent Aite Group study believe synthetic identity fraud is a bigger challenge than identity theft.

Application fraud

When criminals apply for a new account or service using a stolen identity or synthetic identity, it's known as application fraud. These accounts are opened with the sole intent to commit fraud, which usually occurs within the first 90 days of account opening.

According to the latest data from Aite Group, 37 percent of consumers — that's nearly 4 out of every 10 consumers — have been a victim of application fraud in the past two years, from 2018 through 2020.² The study revealed the most common forms of application fraud are for new checking accounts, credit card accounts and mobile phone accounts. Surprisingly, more than half of the victims identified the fraudster as someone they know, like a family member, friend or caregiver.



4 out of every **10**
consumers — have been a
victim of application fraud

Here's another shocker.

In 2020, there was an eye-popping 2,920% spike in fraudulent applications for and receipt of government benefits, according to the Federal Trade Commission.⁹ It's likely pandemic-driven, but it proves how quickly criminals can pivot their operations and successfully attack vulnerable new targets.



2,920%
spike in fraudulent applications

Account takeover fraud

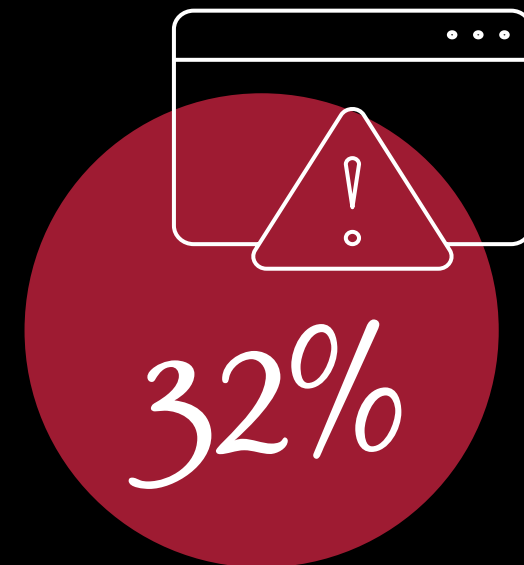
Numbers like this keep executives and analysts awake at night: account takeover fraud exploded by 72 percent in 2019, according to Javelin.¹⁰ This type of fraud occurs when criminals gain access to an account—be it a bank account, credit card account or other account—through data breaches, malware or phishing. They then use the account information to contact call centers and make changes to account, giving themselves full control of the account, while also enabling them to fraudulently apply for additional accounts and loans with the business.

Here's the scary part. In account takeover fraud, a large portion of the fraudulent activity, 40 percent, happens on day one.¹⁰

Looking ahead, as opportunistic fraud associated with the pandemic—think: diverting government stimulus checks and benefits—winds down, fraud experts believe criminals will refocus their efforts on account takeover fraud and application fraud, causing both fraud types to rise in prevalence in coming months and years.



40 percent of fraudulent activity happens on day one.



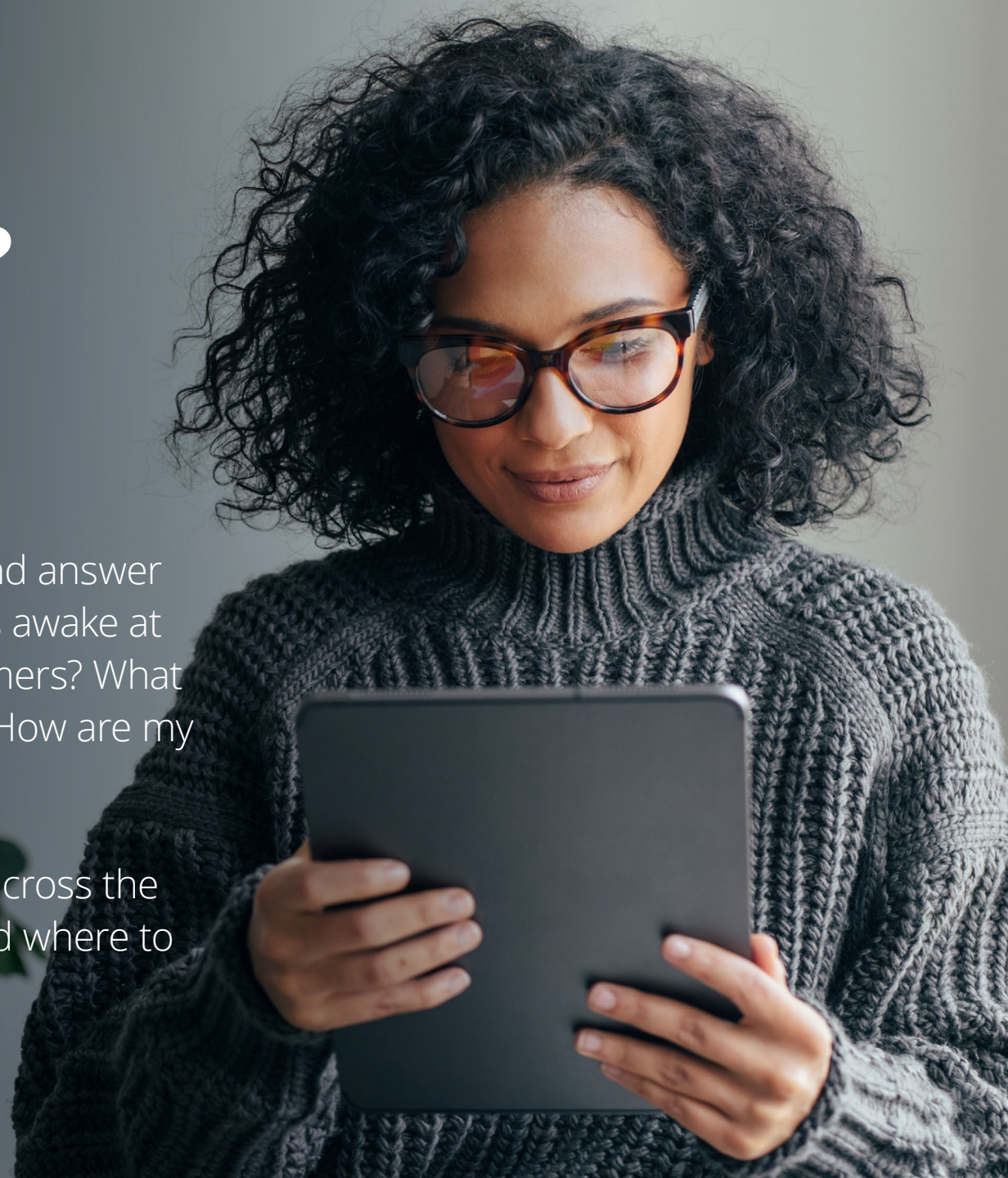
From pre-pandemic through 2020, 32 percent of surveyed fraud executives reported an ***uptick in account takeover attacks of 10 percent or more.***

Aite Group, Key Trends Driving Fraud Transformation in 2021 and Beyond.
December 2020

What do these trends mean to your business? Your customers?

Next, in Chapter 2, we'll dive into the customer journey and answer a few of the burning questions that keep fraud executives awake at night. How is fraud impacting my business and my customers? What touchpoints are most vulnerable to what types of fraud? How are my fraud strategies impacting the customer experience?

You'll see the bigger picture of fraud, how it's connected across the business and get fresh ideas and insights around how and where to focus your fraud mitigation strategy moving forward.



Learn more

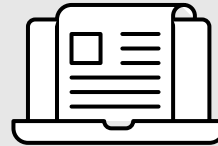


404.885.8500 • equifax.com/business/prevent-fraud



Visit us today.

[Learn more](#)



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

[Equifax Insights](#)



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

[Equifax](#)

Sriram Tirunellayi

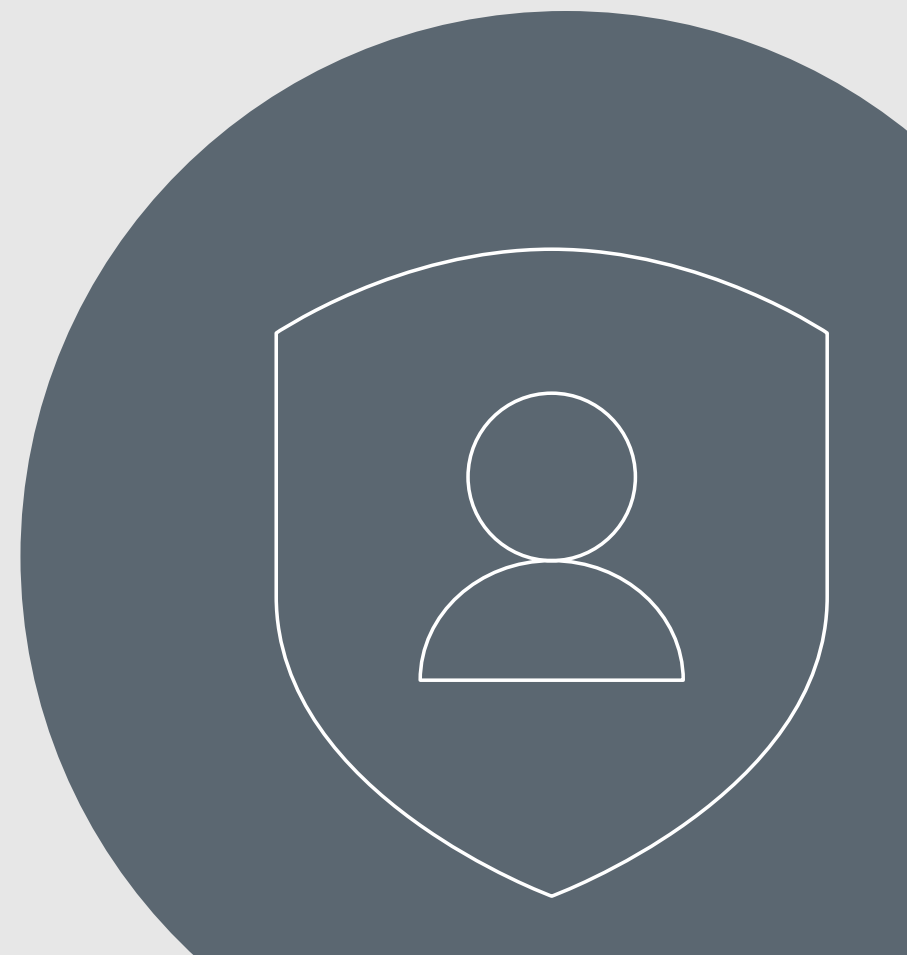
VP of Data and Analytics,
Equifax

Cori Shen

Data Science and Analytics
Director, Equifax

References

1. https://public.tableau.com/profile/federal.trade.commission?utm_source=govdelivery#!/vizhome/COVID-19andStimulusReports/Map
2. Aite Group: U.S. Identity Theft: The Stark Reality. March 2021
3. Javelin: 2020 Identity Fraud Study: Genesis of the Identity Fraud Crisis. April 2020
4. PwC's Global Economic Crime and Fraud Survey 2020
5. <https://www.fool.com/the-ascent/research/buy-now-pay-later-statistics/>
6. <https://www.businessinsider.com/buy-now-pay-later-ecommerce-financing-and-consumer-credit#:~:text=Buy%20Now%20Pay%20Later%20Market&text=The%20pandemic's%20impact%20and%20BNPL's,estimated%20to%20record%20in%202018.>
7. <https://www.americanbanker.com/news/credit-cards-seek-a-role-in-preventing-buy-now-pay-later-defaults>
8. <https://aitegroup.com/report/synthetic-identity-fraud-diabolical-charge-offs-rise>
9. <https://public.tableau.com/profile/federal.trade.commission#!/vizhome/ConsumerSentinel/Infographic>
10. <https://www.javelinstrategy.com/press-release/identity-fraud-losses-increase-15-percent-consumer-out-pocket-costs-more-double>
11. Aite Group. Key Trends Driving Fraud Transformation in 2021 and Beyond. December 2020.





404.885.8500 • equifax.com/business/prevent-fraud