EQUIFAX®

Digital Fraud Trends

Contents

Introduction

In recent years, digital transactions have increased exponentially around the globe. And there are a couple reasons for this shift. First, the pandemic era forced businesses and consumers alike to connect in new ways — via online interactions. And the trend has yet to fade away.

Second, because of the shift in online interactions, businesses have had to adopt new technologies — such as apps, ecommerce sites, social media, and other digital platforms. Customers can now engage with businesses across a variety of channels. And in many cases, they expect this level of ease when engaging with a brand.

Yet, as digital interactions continue to increase, so do fraud vectors. Attacks are becoming more sophisticated as newer, advanced technologies arise. It's a never-ending battle.

All that to say, businesses are in a tough spot — between managing consumer demand, protecting their assets, and finding opportunities to grow. In this market, you need to know what you're up against.

Methodology

The Digital Fraud Trends 2024 report analyzes data from the Equifax global data network, which includes insights from approximately 65 billion transactions, 16,000 merchants, 250 geographical locations, and over 75 industries. The data used in this report was collected from years 2020 to 2023.

65 billion transactions

250 geographical locations

16,000 merchants

over 75 industries

The digital landscape

Fraud has been an ongoing issue for years. According to a recent Ethoca report, in 2023 alone, fraud losses for digital payments totaled $20 billion. Global card-not-present (CNP) fraud losses are projected to grow, reaching $28.1 billion by 2026[1]. That's a 40% increase from 2023.

On top of that, new fraud vectors are continually popping up — from account takeover attacks to refund fraud to AI scams. And with these waves of new fraud attacks come a hefty price to pay in chargebacks. In 2023, the global chargeback volume was reported at more than 237 million transactions[2]. By 2026, predicted volumes could reach 337 million.

[1,2] Ethoca. (2024). 2024 Outlook: Strategic insights for issuers and merchants. https://hs.ethoca.com/2024-payments-outlook-report

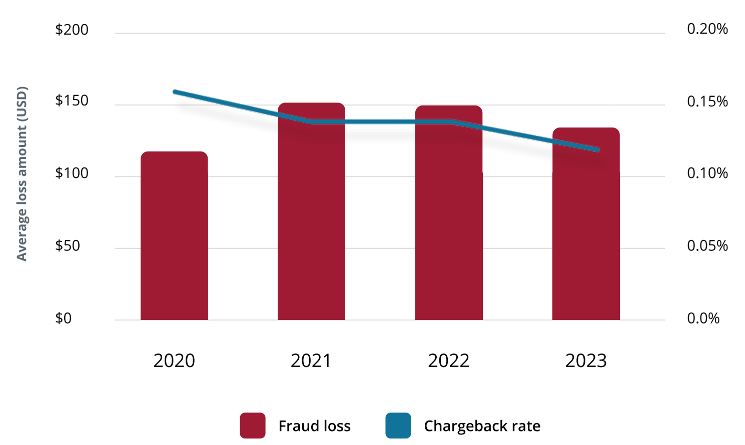
The silver lining

The growth of fraud and chargebacks is concerning, to say the least. However, there is some hope. These losses are preventable — as long as you have the right solution in place.

If we look at our merchant data, it's clear. Despite the increases in fraud over the past few years, the chargeback rate for businesses using our Payments Fraud solution continues to decrease. And though fraud losses soared in 2021, our customers began to see those losses slowly taper off.

Fraud solutions can help you securely navigate the digital marketplace, ensuring a safer shopping experience for your customers.

Fraud providers keep chargeback rates low and steady



Year over year, Equifax Payments Fraud customers experience a **6.5%** decrease in chargeback rate

Fraud trends in 2024

We're also seeing a shift in the way that fraud is conducted. The days of fraudsters sitting behind a computer carrying out attacks are no longer our reality. Fraudsters can commit a variety of attacks from anywhere at any time, thanks to mobile devices. Looking at our merchant data, we can clearly see the shift. Since 2020, mobile fraud has increased 15% year over year (YoY). Meanwhile, fraud committed on a desktop computer has steadily gone down 5% YoY.

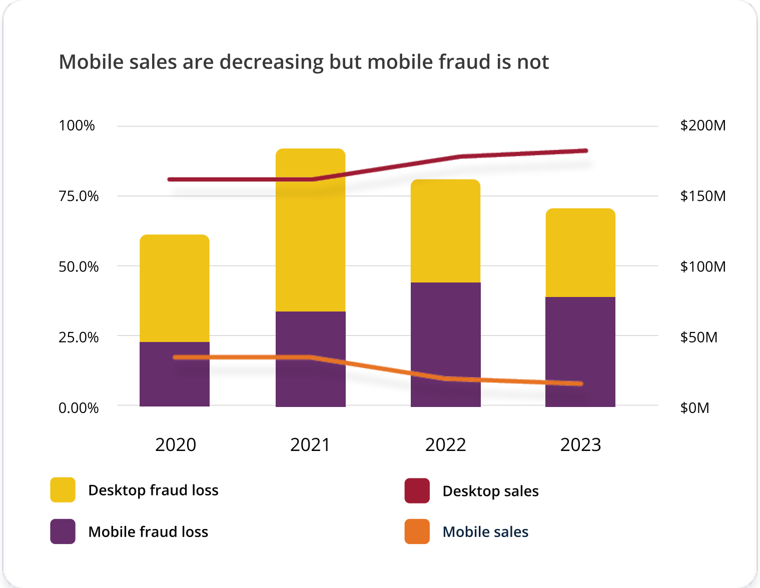
Between years 2021 and 2022, mobile fraud increased **44%**

Mobile sales and fraud

What's interesting about the rise in mobile fraud is that mobile sales have been declining since 2021. However, despite the decrease in sales, fraud losses are up 19% YoY. Meanwhile, desktop sales are up and fraud losses are down.

Part of this shift could be tied to the fact that mobile app security is often neglected by developers — making apps more vulnerable to fraud. And it's easy to see why fraudsters would target mobile apps. They store an immense amount of valuable consumer data.

More than ever it's important to build fraud protection into every aspect of your business — especially with digital interactions.



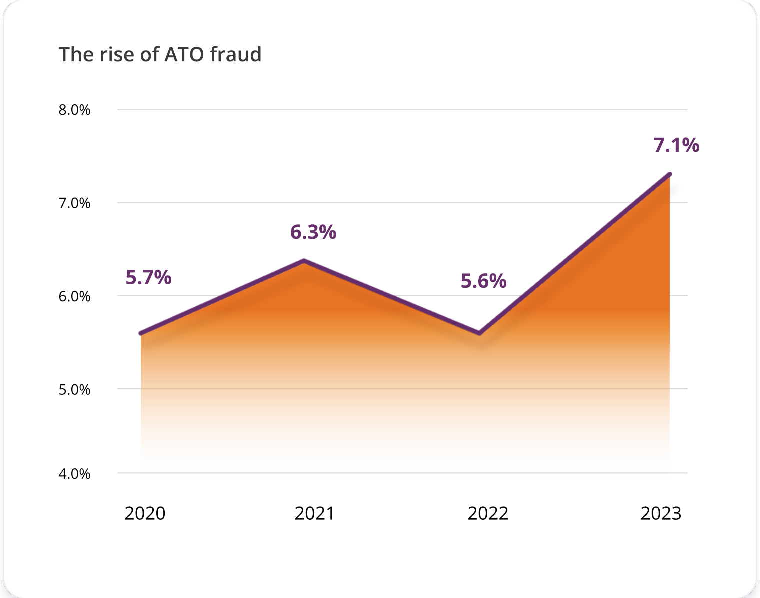
Mobile sales are decreasing but mobile fraud is not

In 2022, **desktop** fraud losses were **down 16%**, while mobile fraud losses **increased by 52%**

Account takeover fraud

Lack of mobile app security lends itself to one of the top fraud attacks going on today: account takeover (ATO) fraud. In our analysis of our merchant data, we've seen the ATO fraud rate increase 8% globally YoY.

The problem is fraudsters are becoming better at circumventing controls — using tools like generative AI to impersonate customers and hack into accounts. And this issue is likely to get worse if businesses don't start taking preventative measures now to protect consumer accounts.



From 2022 to 2023, ATO fraud **increased 26%**

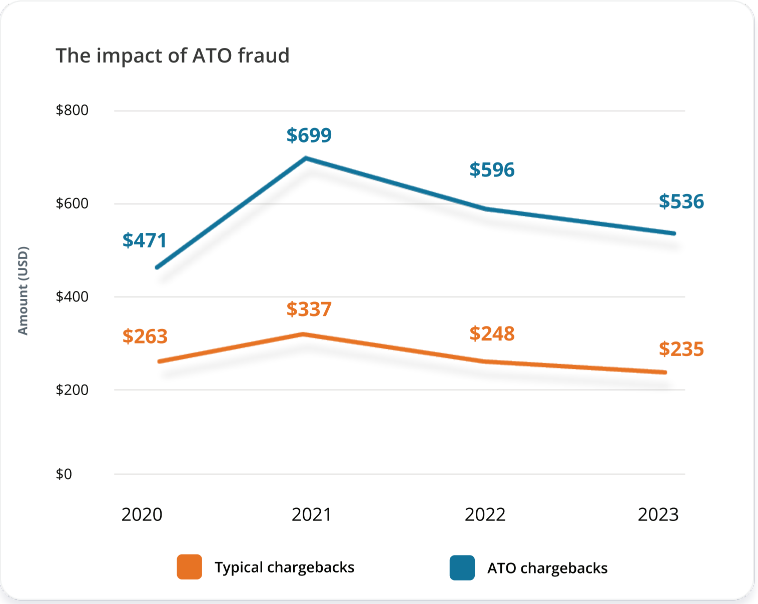
The impact of account takeover attacks

Why should you really care about ATO fraud? Because you have more to lose from not protecting consumers' accounts than from investing in protection. According to our merchant data, over a four-year period, the average loss for chargebacks due to an ATO attack is $576. For typical chargebacks, the average loss is $271.

Fraudsters can do a lot of damage when they have access to customer information — from making unauthorized purchases to selling card numbers online.

Customers put a lot of trust in businesses to keep their account safe. And when that trust is broken, they will seek some sort of justice — whether that's disputing purchases, writing bad reviews of your business, or telling their friends not to do business with you.

ATO chargeback losses are **76% higher** than typical chargebacks



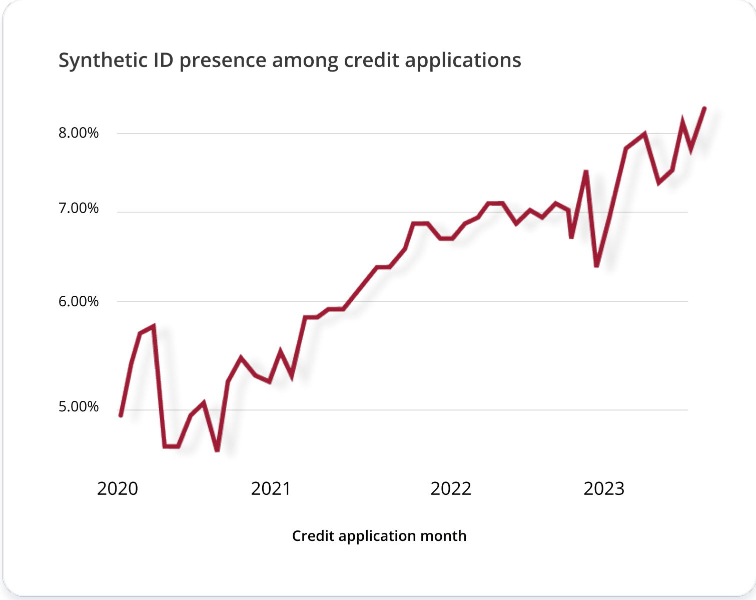
Synthetic identity fraud

Chances are, you've heard of synthetic identity fraud by now. It's spreading fast amongst the fraud community and could be your biggest underlying threat.

Synthetic identities are difficult to spot because they look legitimate, being made up of real information — like social security numbers — and fake names or email addresses. Often, Fraudsters target money lenders because the rewards are so high.

According to Equifax credit application data, this threat has had a major spike in popularity over the past few years, with a 14% growth rate YoY. Scary. But why is this threat so dangerous?

Because it's nearly impossible to trace the fraud back to a fraudster. So, all the losses you accrue are likely unrecoverable.



Over the course of four years, synthetic ID risk **increased nearly 50%**

Social security number recycling

One method fraudsters use to conduct synthetic ID scams is to steal and reuse social security numbers (SSN) — a tactic known as SSN recycling. After receiving money, fraudsters will reuse a SSN, create a brand new fake identity, and reapply for credit or a loan.

To make matters worse, fraudsters typically collect and share these SSNs amongst one another, creating a network of crime. Wide-scale eradication of this threat is unlikely to happen. So it's up to you to screen for synthetic IDs and prevent them from entering your business ecosystem.

Recycled SSNs are **3X more** likely to appear on credit applications

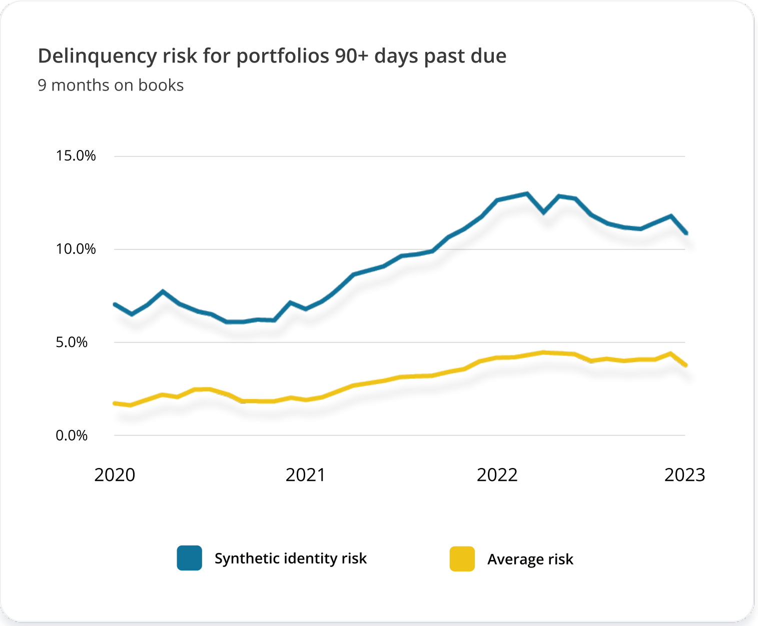
Delinquency risk for synthetic IDs

Not all synthetic accounts will default. Some come from individuals who intend to pay back loans but can't get a loan with their own information or credit score. However, overall, synthetic IDs have a much higher risk of defaulting on loans than typical portfolios — from threefold to fivefold.

In our analysis of Equifax credit application data, we found that among personal loans, synthetic identities tend to default within the first six to nine months of the loan. For credit cards, a good portion of synthetic IDs default within the first nine months. However, some may take anywhere from 24 to 36 months or more to go bad.

Ultimately, it doesn't matter if an account defaults in month 6 or 36. Since synthetic IDs are more likely to default, it's important to put protections in place to prevent them from existing altogether.

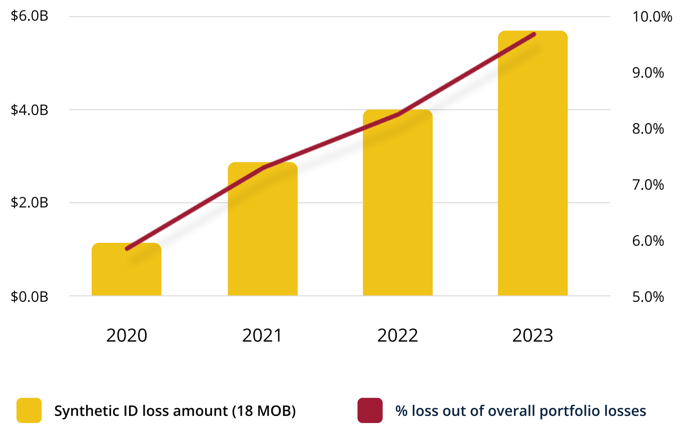
Over a 9-month average, synthetic identities are **three to five times** more likely to fall delinquent on loans



Synthetic ID loss

Not only are financial losses more likely to happen with portfolios made up of synthetic IDs, those losses are incredibly high. And they're drastically increasing each year. Based on our analysis, it's likely that this trend will only continue to grow as more avenues emerge that allow fraudsters to create these identities.

A growing portion of total portfolio loss is from Synthetic IDs



From 2022 to 2023, synthetic ID losses increased by nearly **50%**

YoY, Equifax Payments Fraud solution stops **17%** more fraud than banks

How fraud is prevented

Fraud is growing. Fraud vectors are increasing. Who's responsible for stopping all this risk?

Ultimately, merchants are responsible for protecting their businesses and customers. But in reality, it's a collaborative effort between issuing banks, merchants, and fraud solution providers.

However, the right balance can be difficult to achieve. Merchants often have their own internal fraud processes. Usually, that means manual reviews — which can be time-consuming and laden with errors.

And issuing banks have a tendency to be strict when it comes to fraud decisioning. They often decline more transactions than necessary for a variety of reasons — lack of sufficient data, categorizing a merchant as high risk, and more.

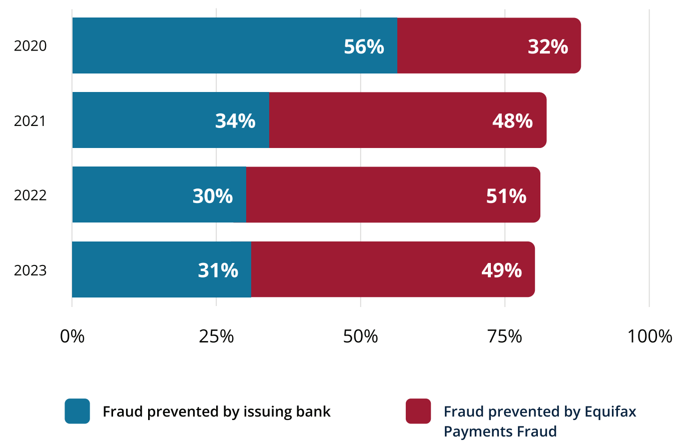
These older methods of fraud prevention haven't gone away. However, there's a major shift happening in the role they play. Fraud solutions are taking over as the preferred method of risk mitigation.

And the proof is in the data. From our analysis of merchant data, we can see that over time fraud solutions like our Payments Fraud solution have taken the lead in fraud prevention. In 2020, issuing banks were responsible for stopping 56% of payments fraud. Meanwhile, our solution was taking on only 32% of payments fraud.

Today, those roles have completely switched. Banks are responsible for stopping 31% of payments fraud while our solution stops 49%.

That's because fraud solutions have enormous amounts of data — which improves decision accuracy. And this data can also be used to help inform bank approvals and declines. The fraud technology simply does a better job at identifying what is and isn't fraud. And that's why it should be the preferred method for fraud prevention.

The solution: fraud technology



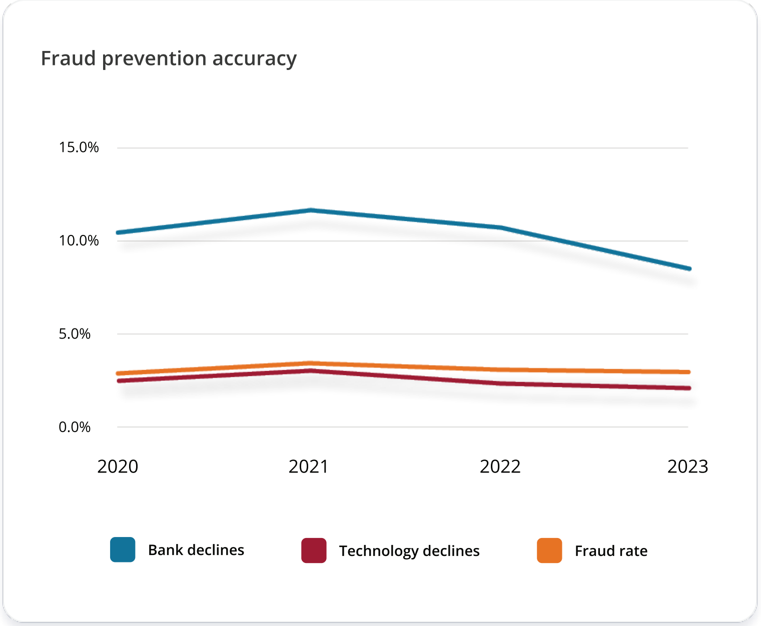
Fraud prevention technology surpasses other methods in accuracy

Before the wide-spread adoption of fraud technology, businesses relied on a combination of tools to mitigate fraud — including time-consuming manual reviews and pre-authorization declines from banks. However, these methods are outdated.

And it's clear from our analysis that banks simply don't have the data to make accurate fraud decisions. The fraud rate has hovered around 2% to 3% over the past few years. Yet banks have declined significantly more transactions — meaning, they're declining too many legitimate transactions.

Meanwhile, fraud technology has been declining orders at a rate consistent with the overall fraud rate. That's to say, the technology is getting it mostly right almost all the time. Of course, it's impossible for any solution to be 100% accurate because of events — like post-transaction friendly fraud — that are unpredictable.

The reason fraud prevention technology surpasses traditional methods is simple. It's all about data. Technology can collect billions of data points that banks and businesses can't. And with that data, the solution can make more informed decisions on what is and isn't fraud.



On average, the decline rate for banks is **121%** higher than a fraud solution

Conclusion

Fraud is always going to be an issue. But that doesn't mean you have to simply accept it as a cost of doing business. Solutions exist and prevention is possible. Remember that a proactive approach is key. Ideally, you want to build a forward-thinking fraud strategy — one that can solve for a variety of threats and quickly respond to emerging ones.

About Equifax

Equifax is a global data, analytics, and technology company, playing an essential role in the global economy by helping financial institutions, companies, employers, and government agencies make critical decisions with greater confidence. From verifying identities and preventing fraud to fighting chargebacks and recovering lost revenue, we can help your business overcome today's most challenging issues.

The information presented herein is for general informational use only. Neither Equifax nor any of its affiliates make any express or implied representation or warranty as to the accuracy or completeness of the information contained herein. Equifax and its affiliates expressly disclaim any and all liability which could be based in whole or in part on such information, errors therein or omissions therefrom. This information is qualified in its entirety by the footnotes, assumptions and other qualifying statements contained herein. This information should not be relied upon in making any financial decision or otherwise. Such information is presented as of the date hereof only and is subject to change without notice. Equifax undertakes no responsibility to update or supplement the information contained herein.