Identifying and Navigating Top Fraud Risks

How to keep your business and your customers safe from fraud.

PayPal

Contents

Get ahead of global fraudsters

Cybercrime is everywhere. It costs the world nearly US$1 trillion per year[1] and, unfortunately, no one is immune. Fraudsters target every sector in every country, regardless of whether the organisation is a local small business or a large, multi-national enterprise.

But, by learning which types of attack are most likely in any situation, businesses can be better prepared to anticipate and fight fraud.

1, 2. Center for Strategic & International Studies (2020), The Hidden Costs of Cybercrime **3.** Cybersource (2021), 2021 Global Fraud Report **4.** Payments Dive (2021), E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds
5. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/Retail Report **6.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report **7.** South China Morning Post (2022), Hong Kong online scam victims report losing HK$3 billion...

Why cybersecurity should be your top priority

Fraud and cybercrime are bad for business. Obviously, there is the potential loss of revenue or goods maliciously acquired. But there is also the huge cost of dealing with attempted fraud – over 3 times as much as the revenue lost.[8]

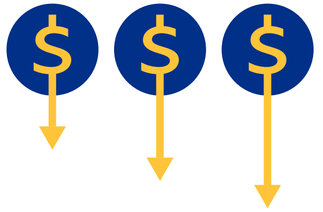
When your business suffers from payment fraud, it can lead to 3 types of losses.

- The goods or services you provided have been stolen, so you have a direct loss and need to pay to replace your inventory.
- The real cardholder wants their money back, along with a chargeback fee levied by the payment processor, which means a writeback of revenue plus additional operating costs.
- You have to devote time and resources to handling fraud and complaints from genuine customers whose accounts have been hijacked. This results in higher operating costs for your business.

Companies can also suffer reputational damage from a large-scale or well-publicised attack. And even if attacks don't catch the public eye, a high rate of chargebacks or other fraud attempts can result in the business being considered as higher risk by their payment provider, leading to more onerous requirements and higher processing costs.[9]

Data breaches or inadvertently processing fraudulent transactions can lead to sanctions or fines from regulatory authorities, including anti-money-laundering (AML) regulators.

This guide looks at some of the most common types of fraud in different sectors and how to deal with them.



There is also the huge cost of dealing with attempted fraud —

over 3x

as much as the revenue lost.[8]

8. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/Retail Report **9.** Forbes (2021), High-Risk Merchant Account: What It Is And How It Works

Common types of payment fraud

Account takeover (ATO) fraud

Account takeover is a form of identity theft in which criminals gain access to a genuine customer's account to make unauthorised purchases and/or to steal the personal and payment details stored in the account. Common ways to do this include:

- **Credential stuffing —** Bots bombard account logins with thousands of username/password combinations, often purchased in bulk on the dark web.
- **Phishing and other social engineering —** Customers are tricked into revealing their credentials, often through fraudulent emails or phone calls.

Card testing

Here, criminals test large volumes of stolen card details to see if they are still valid. They typically use bots or computer scripts to make large amounts of low-value transactions. Successful cards are then used for larger purchases or sold on to other fraudsters.

Card-not-present (CNP) fraud

CNP fraud occurs when a card is used to make a purchase but the card is not presented. Originally, this meant phone and mail-order purchases but today it covers all eCommerce purchases. CNP fraud comes in two forms, traditional CNP fraud using stolen card details and friendly fraud (see below). Both types result in the genuine cardholder filing a chargeback.

Friendly fraud

So-called friendly fraud occurs when the cardholder disputes a legitimate transaction. Sometimes this occurs when they don't remember making a purchase or don't know that a family member used their card to make a purchase. At other times, the purchaser might regret an impulse purchase or have forgotten to cancel a subscription and decides to file a chargeback request rather than admit to a mistake. Friendly fraud also occurs when a customer makes a false "goods not delivered" claim.

Chargeback fraud

When a cardholder disputes a charge, the bank or card company reverses the charge and levies a chargeback fee on the merchant. Chargebacks can arise from problems with the transaction (perhaps the goods were not delivered or an error was made in charging the card). They can also be requested by the legitimate cardholder when they spot a fraud. While many chargebacks can be genuine, there is also a growing trend of fraudulent chargeback requests.

Synthetic identity fraud

This is one of the fastest-growing types of financial fraud. Criminals create a false identity based on stolen or wholly fictional personal details and then take the time to slowly build a credit history for the made-up identity. With a valid-looking ID, they can then apply for credit cards or loans and spend to the limit before disappearing. This type of fraud is difficult to detect until it's too late.

The fraud profile in online retail / eCommerce

The rapid, global growth in eCommerce over the past couple of years has been followed by a big increase in all types of payment fraud attack.

Friendly fraud and card testing are the most common attacks globally.[10] Online retailers report rises in every type of attack including chargebacks and friendly fraud.[11]

More than half of merchants surveyed reported increases in identity and account-related fraud such as synthetic identity fraud, account takeovers, identity theft and new account fraud.[12] 59% of the merchants surveyed also reported an increase in card-not-present fraud.[13]

According to fraud experts Arkose Labs, 1 in every 4 retail transactions was an attack.[14]

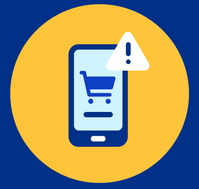
It's no surprise that eCommerce sellers everywhere, of every scale, are viewing fraud as a serious challenge:

3 in 5

merchants feel that revenue loss from payment fraud has a substantial or significant effect on their business.[15]

3 in 5

merchants also feel that lost productivity due to payment fraud has a substantial or significant effect on their business.[16]



9 out of 10

merchants now consider managing eCommerce fraud "very or extremely important" to their overall business strategy.[17]

1 in 5

merchants say that customer data security is a critical challenge.[18]

10, 17. Cybersource (2021), 2021 Global Fraud Report **11, 12, 13, 15, 16, 18.** FIS Worldpay (2021), Global Payment Risk Mitigation **14.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report

The fraud profile in online gaming

With high transaction volumes, customers' demand for fast and friction-free transactions, and US$50 billion total value of global, in-game assets,[19] the world of online gaming and esports has always been an attractive target for fraudsters.

Just the sale of stolen Fortnite accounts is estimated to generate US$1 billion per year for criminals.[20]

The problem for gaming companies is that launching fraud attacks is extremely profitable for cybercriminals. As Arkose Labs points out, bot attacks can be launched for just US$15 per day and captured accounts can be resold for up to US$3,000.[21]

According to Arkose, online gaming was the most attacked industry in 2020[22] and while overall attacks levelled off in 2021, the types of attacks diversified.[23]

The top types of fraud attack in the online gaming sector include:

- **Account takeover attacks —** 2 out of every 3 attacks in 2021 targeted user logins.[24] Attack methods include credential stuffing where bots are deployed to constantly try different combinations of username and password. Once accounts are compromised, in-game assets, payment and personal details can all be stolen and sold.
- **Phishing and other social engineering fraud** which generally lead to either account takeover or theft of payment and personal details.
- **Friendly fraud** is common in the sector. It occurs when customers dispute a legitimate transaction. This can happen because they don't remember the transaction, there is confusion with a family member or they regret an impulsive purchase.
- **Card testing fraud** is also common in the games sector because of its high transaction volumes and often low transaction values — ideal for hiding card-testing activity.

The APAC region generates the most revenue for the global gaming industry with the number of mobile gamers reaching 250 million in 2021.[25] China, Japan, South Korea, Indonesia and Australia are all in the global top 10 for mobile game revenues.[26] At the same time, across the APAC region, technology and gaming companies are the primary targets for fraud attacks.[27]

19. Intellicheck (2021), How companies can prevent fraud in online gaming **20.** Business Insider (2020), Stolen Fortnite accounts are being sold on the black market... **21, 22.** Arkose Labs (2021), How to Level Up in the Fight Against Online Gaming Fraud
23. Arkose Labs (2021), Fraud in Online Gaming: A Midyear Snapshot of 2021 Attack Trends **24, 27.** Arkose Labs (2022), 2022 State of Fraud & Account Security Report **25.** Transperfect (2021), What Does Global Gaming Industry Growth Look Like in 2021? **26.** Newzoo (2021), Global Mobile Market Report 2021

The fraud profile in SaaS and services businesses

According to Arkose Labs, technology businesses were 5 times more likely to suffer a fraud attack in 2021 compared to the previous year.[28]

SaaS, and any sort of subscription business, is especially vulnerable to fraud attacks because every account has payment details associated with it.

Technology businesses were **5x** more likely to suffer a fraud attack in 2021 compared 2020.[29]

- **Account takeover (ATO) fraud** is a common threat for SaaS business. Once accounts have been compromised, they are used to buy services and goods or sold on to other criminals.
- Using stolen card details to open fake accounts and make purchases **(CNP fraud)** and using fake accounts to abuse free trial offers are also common in the SaaS space.
- **Chargebacks** are another big challenge in this sector. In fact, the software industry has the highest average chargeback-to-transaction ratio at 0.66%.[29] Some of these are innocent, with people forgetting what they've subscribed to, but many others are fraudulent.

28. Arkose Labs (2022), 2022 State of Fraud & Account Security Report **29.** Expert Market (2021), Chargeback Fraud Statistics 2022

How to prevent payment fraud

Frustrating account takeover attacks

Some payment providers such as PayPal offer multi-factor authentication (MFA) or two-factor authentication (2FA) . It can be a powerful way to head-off both credential stuffing and the use of credentials stolen in phishing attacks. In fact, two-factor authentication was cited as "very important" by nearly half of all merchants.[30]

When MFA/2FA is enabled, your customer is asked to provide an additional form of authentication (such as a one-time numeric code) that is sent to their pre-registered mobile phone or email account. This prevents fraudsters from simply using stolen credentials, as they also need access to the real owner's mobile device or email.

Because the first step in an account takeover (using bots to run credential stuffing attacks) is often automated, a simple step like introducing CAPTCHA technology — which requires human intervention — can also be effective.

Detecting and dealing with card testing

These attacks involve large volumes of small transactions in a short space of time. In high-volume scenarios like eCommerce or online gaming, card-testing transactions can easily go unnoticed and, without protection, sellers can quickly suffer a wave of chargebacks because of an attack. Card testing attacks can also impact a merchant's infrastructure availability with excessive failed authorisation attempts.

PayPal uses machine learning algorithms and real-time decision-making to help differentiate between good and bad transactions and quickly identify fraudulent patterns like card testing. PayPal compares historical trends and transaction information such as IP address, device type and ID, email address and other information.

Machine learning is only as good as the data set it is learning from, an area where PayPal has a strong advantage due to our two-sided network. With over 400 million consumers and 30 million merchant accounts across a wide range of sectors, PayPal has a wealth of data on consumers and risk profiles. This insight into both the merchant and consumer sides of the transaction helps allow us to make the call on a true or fraudulent transaction for even the most sophisticated fraud behaviour.[31]

Over **400M consumers** and **30M merchants** use PayPal.[31]

30. FIS Worldpay (2021), Global Payment Risk Mitigation **31.** PayPal (2020), How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates

Reducing card-not-present (CNP) fraud

With CNP fraud, the best bet is to request as much information as you can from the payer. This includes asking for the CVV code and implementing fraud prevention measures like 3D Secure (3DS) and Multi-Factor Authentication (MFA).

Again, payment providers like PayPal that use machine learning on real-time data can help reduce instances of CNP fraud. PayPal's pioneering use of network tokenization[32] makes it difficult for criminals to make fraudulent use of stolen card details.

Fighting friendly fraud

Friendly fraud (also called first-party fraud) is common in the eCommerce and gaming sectors. It can be difficult to detect and to prove. However, maintaining good records and policies that prove goods or services were legitimately ordered, shipped and received can help you refute false claims. One example of this would be requiring a signature on receipt of goods.

Many friendly fraud claims start out as valid transactions so having a clear and generous returns policy, great customer service and good communications can also help prevent some customers from falsely claiming a chargeback.

Always requesting the card's CVV value and implementing 3D Secure also makes it more difficult for people to commit friendly fraud.

Businesses may be able to benefit from PayPal Seller Protection.[33]

Reducing chargeback fraud

Because nearly all payment fraud results in chargebacks, improving your overall fraud defences will help to reduce chargeback fraud.

One of the best ways to reduce chargeback fraud is to work with a payment processor like PayPal that uses advanced fraud prevention technology. Fraud techniques are always evolving, so you need a fraud prevention solution that constantly evolves, based on real-time data, to meet the threat.

Preventing synthetic identity fraud

Synthetic identities succeed because many financial institutions use unsophisticated and/or automatic scoring systems to offer credit. Leveraging greater volumes of data, including third-party data, can often reveal the inconsistencies that are common in fake IDs.

The data from PayPal's large, two-sided network of merchants and consumers is a rich source for our machine-learning models of fraud detection.

32. PayPal (2020), How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience **33.** Terms and Conditions apply

How PayPal can help manage fraud risk

PayPal's payments technology, developed over 20 years, is designed to reduce the risk of fraud while boosting customers' confidence to spend.

Around the world, the PayPal brand is recognised and trusted. Customers appreciate the fact that their personal details are never shared. They may benefit from a payment experience that is designed for the easy and secure convenience today's buyers expect.

With PayPal, sellers can offer a wide range of payment methods (including alternative local payment methods) with a single integration. With PayPal, sellers can offer a wide range of payments methods through one integration making it easier to manage and orchestrate payments centrally.

Businesses can also benefit from PayPal Seller Protection on eligible transactions[34] and fraud prevention standards such as 3D Secure.

PayPal offers advanced fraud prevention capabilities. Our two-sided network of 400+ million active users worldwide provides a rich source of data which is fed into our machine learning models for more accurate, adaptive, and real-time fraud detection. As a result, there are fewer unnecessary transaction declines and less chance of inadvertently treating your good customers like fraudsters.

PayPal's massive data set of merchants, advanced machine learning techniques and data science expertise also make it faster to identify newly trending fraudulent activities and to act accordingly across all other merchants on the network.

Our global relationships with banks, acquirers and regulators also place us in a good position to identify potential fraud before it happens.

For enterprises, PayPal has two fraud prevention offerings:

Fraud Protection:
Fraud Protection is an out-of-the-box toolkit built into the PayPal Commerce Platform and Braintree, designed to help provide merchants with more visibility and control over the transaction decisioning process.

Fraud Protection Advanced:
Built into Braintree, Fraud Protection Advanced helps enable a merchant's fraud team(s) to identify and investigate suspicious transactions, analyse patterns, and uncover key insights to mitigate fraud losses.

Learn more about how PayPal helps enterprises manage risk and maintain compliance

Learn More

The results of PayPal's advanced risk management can include:

- Fewer chargebacks
- Lower false positive rates
- Less customer friction
- Lower fraud losses
- Improved operational efficiency
- Streamlined customer experiences

34. Terms and Conditions apply

References

1. Center for Strategic & International Studies (2020), The Hidden Costs of Cybercrime
2. Center for Strategic & International Studies (2020), The Hidden Costs of Cybercrime
3. Cybersource (2021), 2021 Global Fraud Report
4. Payments Dive (2021), E-commerce fraud to surpass $20B in 2021, an 18% jump over last year, report finds
5. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/ Retail Report
6. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
7. South China Morning Post (2022), Hong Kong online scam victims report losing HK$3 billion...
8. LexisNexis (2020), 2020 True Cost of Fraud Study – E-Commerce/ Retail Report
9. Forbes (2021), High-Risk Merchant Account: What It Is And How It Works
10. Cybersource (2021), 2021 Global Fraud Report
11. FIS Worldpay (2021), Global Payment Risk Mitigation
12. FIS Worldpay (2021), Global Payment Risk Mitigation
13. FIS Worldpay (2021), Global Payment Risk Mitigation
14. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
15. FIS Worldpay (2021), Global Payment Risk Mitigation
16. FIS Worldpay (2021), Global Payment Risk Mitigation
17. Cybersource (2021), 2021 Global Fraud Report
18. FIS Worldpay (2021), Global Payment Risk Mitigation
19. Intellicheck (2021), How companies can prevent fraud in online gaming
20. Business Insider (2020), Stolen Fortnite accounts are being sold on the black market...
21. Arkose Labs (2021), How to Level Up in the Fight Against Online Gaming Fraud
22. Arkose Labs (2021), How to Level Up in the Fight Against Online Gaming Fraud
23. Arkose Labs (2021), Fraud in Online Gaming: A Midyear Snapshot of 2021 Attack Trends
24. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
25. Transperfect (2021), What Does Global Gaming Industry Growth Look Like in 2021?
26. Newzoo (2021), Global Mobile Market Report 2021
27. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
28. Arkose Labs (2022), 2022 State of Fraud & Account Security Report
29. Expert Market (2021), Chargeback Fraud Statistics 2022
30. FIS Worldpay (2021), Global Payment Risk Mitigation
31. PayPal (2020), How Data Science, Machine Learning and Artificial Intelligence Lead to Higher Authorization Rates
32. PayPal (2020), How Network Tokenization Leads to Higher Authorization Rates and a Better Customer Experience
33. Terms and Conditions apply
34. Terms and Conditions apply