
PayPal
HOW
TO INCREASE REVENUE
WITHOUT SACRIFICING
SEAMLESS CHECKOUT

Overview

Nearly every merchant has the same end goal: to increase revenue, which often requires an organization to rethink the way it does payments. Is your checkout process fast enough? Are you providing the payment methods your customers are looking for? Is your data security up to par?

Enhancing your checkout process can produce big results. A study of 50 leading websites in the US found that large ecommerce sites could increase their conversions by up to 35% – just by improving their checkout process.[1] There could be as much as $260 billion of recoverable revenue out there, waiting for enterprises to claim it.[2]

Numbers like this are the reason that, when it comes to the checkout experience, business objectives tend to focus on increasing conversion rates. But this way of thinking doesn't take into account the full payments process, including what happens behind the scenes.

Ecommerce revenue is often lost to fraudsters and hackers. Excessive interchange fees and high decline rates can erode more revenue, even on legitimate transactions. But enterprise merchants who are willing to look in the right places – and work with the right payments partner – can put a stop to these drains on their revenue.

> Ecommerce revenue is often lost to fraudsters and hackers. But with the right payments solution, it doesn't have to be.

How can revenue be lost?

Enterprise merchants don't have it easy. Shopping cart abandonment rates average nearly 70% across industries.[3] 90% of customers say brands fail to meet their customer experience expectations.[4] To drive conversions and help earn customer trust, organizations must look at three key factors.

KEY FACTORS:

Fraud

Increased interchange fees

Declines

Fraud

One primary way enterprises lose revenue is through fraud – and it's on the rise. Fraudsters are targeting more types of ecommerce merchants than ever before, and their methods are becoming more sophisticated. Plus, the rise of mobile presents even more opportunities for online fraud.[5]

84% of businesses believe better customer recognition could mitigate fraud

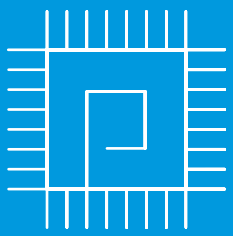
55% of customers don't feel brands recognize them accurately

57% of companies reported higher year-over-year fraud losses from 2018 to 2019

Infographic source:
2020 Global Identity and Fraud Report, Experian, January 2019.

Despite these numbers, the same report found that only 67% of businesses think that advanced techniques like machine learning and AI are important to help prevent fraud.[6] But leading organizations know they must adopt the latest technologies to keep up with emerging fraud trends.

Leading organizations will adopt the latest technologies to keep up with emerging fraud trends.



Online payments are no longer anchored to a desktop computer – or even to a single location. In today's payments landscape, consumers make purchases from multiple devices, anywhere in the world. And while many enterprise merchants think they've caught up with the mobile payments trend, they may be missing one vital thing: security.

Traditional fraud detection systems flag suspicious activity by relying on rule-based filters that need to be updated manually. But they often have two fatal flaws:

1. Flagging too many cases, creating false declines and reducing authorization rates.
2. Missing new fraud trends because the rules they are following don't recognize them.

With consumers on the move and on different devices, it's harder than ever to connect individuals to their transactions. By the time an organization recognizes activity that is legitimately suspicious and changes the rules to detect it, fraudsters may have already moved on to their next scheme. Enterprises must make the switch from outdated fraud detection systems that use static data points and can't adjust to the ways modern consumers pay.

Machine-learning models work together with rules-based systems to help detect changing fraud patterns.

Top fraud solutions leverage a variety of data, both internal and external, and analyze multiple attributes to validate user identity across locations and devices. And they use machine-learning models that work together with rule-based systems to help detect changing fraud patterns.

A business's risk threshold is always an individual decision, and any fraud strategy must include a system for reviewing each transaction. Through Simility, a PayPal service, PayPal for Enterprise offers advanced fraud protections that can help you make your checkout process secure, as well as a disputes team to help you argue against chargebacks when they do arise.

Modern fraud tools

Flexible, scalable data

The age of Big Data is here. 65% of retailers used POS data mining in 2019, an 8-point increase from the previous year.[7] But it isn't enough to collect data. Enterprises that thrive will take advantage of the latest tools to put that data to work for them. They need datasets that are large and diverse, yet also tailored to their specific needs. And they need a solution that knows how to analyze all that data in a way that helps optimize fraud detection.

PayPal for Enterprise, through Simility, leverages third-party data sources and internal feeds and analyzes multiple device types to help enterprises validate user identities. And our flexible data lake technology stores data in a flat, easily scalable architecture. These top technologies make us a payments partner that can grow with enterprises and adapt to changing needs.

Machine-learning models

Fraudsters learn from their mistakes. Fraud detection systems should do the same if they want to keep up. That's where machine learning can help. Machine-learning models supplement traditional rule-based systems: They use "the rules" for training, but are able to evolve by taking into account the latest data in order to suggest updates to rules or thresholds that humans might have missed.

PayPal for Enterprise uses Simility to test rule performance, continuously review historical data for anomalies, and propose new rules based on the findings. Enterprises can take the information provided by machine learning and adjust their processes to fit changing needs and risk tolerances. It's the help many companies need to begin to strike the fine balance between detecting fraud and providing a seamless customer experience.

Global best practices

If you're doing business outside the US, you should consider enabling 3D Secure. 3D Secure allows the cardholder to set up a password (or other verification process) with their card-issuing bank. When the customer checks out on your website, they simply enter their password to verify the transaction.

3D Secure is important for two reasons:

1. It has the potential to shift chargeback liability from your organization to the card-issuing bank. The details of the chargeback liability shift are outlined in our support articles. (Not all cards are eligible for 3D Secure. If a card is not 3D Secure-eligible, chargeback liability will remain with your company.)

2. Many card-issuing banks outside the US require 3D Secure to be enabled in order to process debit cards. For example, almost all Malaysian banks require 3D Secure to be enabled before a debit card transaction will be approved.

Increased interchange fees

Depending on your credit card mix, your transactions could be downgraded by the card brands (meaning an increase in interchange fees would ensue) for being high risk. One of the most common and preventable reasons for interchange downgrade is not providing billing address information for transactions created by US customers. When the billing address information is not provided, the associated interchange fees may be higher.

One of the most common reasons for US interchange downgrade is not providing billing address information.

Declines

There are two types of declines:

Hard declines

Hard declines occur when there is an irreparable issue with the customer's payment method – for instance, the card has expired. No matter how many attempts the customer makes, their provided payment method will not be accepted.

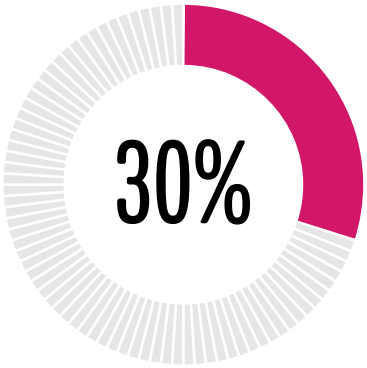
Soft declines

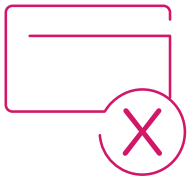
Soft declines come from the card-issuing banks. These cards are connected to a valid account, but there is something preventing the issuing bank from completing the transaction. This is most likely caused by:

1. Insufficient funds
2. The issuing bank's own fraud rules

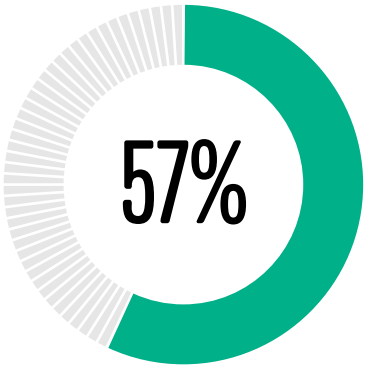
When your payments processor receives a generic soft decline code from the customer's issuing bank, that bank is telling your processor they will not honor this transaction right now. Since this is a temporary issue, merchants can try providing the payment method information again. Just be sure not to retry excessively, as some card brands have strict rules around transaction retries.

Consider This

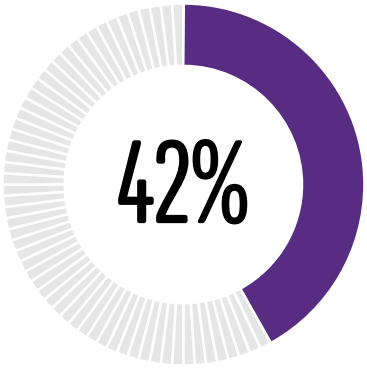




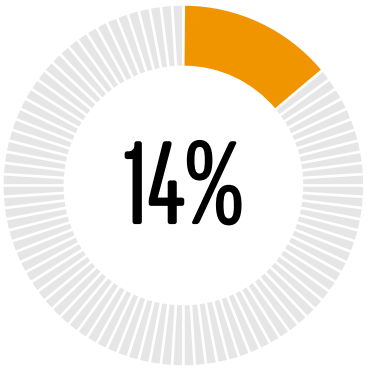
of all shoppers have had a purchase declined



of those were repeat customers



of customers abandon their cart when declined



then take their purchase to a competing merchant

Infographic source:
By the Numbers: How False Declines Cost Merchants, CardNotPresent, December 2018.

The PayPal Difference

Enterprises don't need to compromise security to create a seamless customer experience. Partnering with a payments expert like PayPal can help your business limit declines and fraud, without creating unnecessary friction for customers.

PayPal is the only payments platform that accepts credit and debit, ACH, popular digital wallets, Venmo (US only), and PayPal, all in one seamless integration. Research shows that PayPal is one of the most popular payment methods that many consumers look for when completing a purchase.[8] PayPal One Touch for mobile and desktop makes it possible for even first-time customers to check out quickly.

Beyond the shopping cart, we offer the latest tools to help enterprises adapt to evolving fraud patterns and securely store billing information. And our PCI resources help ecommerce companies stay in compliance and manage interchange fees.

It's time to uncover new revenue streams you may not even know you have. Reach out to us to learn more about making the most of your PayPal integration.

About PayPal

Fueled by a fundamental belief that having access to financial services creates opportunity, PayPal (NASDAQ: PYPL) is committed to democratizing financial services and empowering people and businesses to join and thrive in the global economy.

Our open digital payments platform gives enterprise merchants the confidence to connect and transact in new and powerful ways, online, on a mobile device, in app, or in person. Through a combination of technological innovation and strategic partnerships, PayPal creates better ways to manage and move money, and offers choice and flexibility when sending payments, paying, or getting paid.

Available in more than 200 markets around the world, the PayPal platform, including Braintree, Venmo (US only), and Xoom, enables 281+ million consumers and 24+ million merchants[9] to send and receive money across borders and payment methods.

Click here to learn how PayPal for Enterprise can help you thwart 3 common revenue killers.

Sources:

1 41 Cart Abandonment Rate Statistics, Baymard Institute, updated September 10, 2019.
2 41 Cart Abandonment Rate Statistics, Baymard Institute, updated September 10, 2019.
3 41 Cart Abandonment Rate Statistics, Baymard Institute, updated September 10, 2019.
4 Deliver the CX They Expect, Acquia, July 2019.
5 True Cost of Fraud Study, LexisNexis, 2019.
6 2020 Global Identity and Fraud Report, Experian, January 2019.
7 National Retail Security Survey, National Retail Federation, March 2019.
8 Digital Wallet Adoption, 451 Research, Q3 2019.
9 PayPal Q4 2019 Quarterly and Year End Report.