Charge ahead @ vesta.io

The True Cost of eCommerce Fraud

The sudden growth in online spending has prompted a rise in card-not-present (CNP) fraud

Summary

Online shopping has surged amid the COVID-19 pandemic, and as eCommerce companies have tried to battle the greater threat posed by fraud, many have gone overboard in rejecting good transactions alongside the bad ones, resulting in false declines becoming a more expensive problem than fraud itself. Once a legitimate customer's purchase is declined, not only do merchants lose the sale, but they also often lose the customer for life. This guide delves into how much fraud is really costing merchants and what companies can do to better balance their acceptance and fraud rates.

Introduction

When it comes to eCommerce fraud management, businesses tend to focus on the direct financial hit from chargeback remediation rather than examining their fraud problem holistically. Beyond the financial impact that fraud attacks have on a business, there are a variety of indirect costs that can negatively impact a company's ability to scale.

In this post we'll be looking at the key costs associated with eCommerce fraud, and how businesses can effectively manage their fraud problem to maximize approval rates and eliminate their fraud risk.

Note: This article is based around content that was presented in a recent webinar for Merchant Risk Council, "eCommerce Fraud: It's Costing Merchants More Than They Think". To view that webinar recording, please visit the MRC Website.

Here's what we'll be covering:

1 The current state of eCommerce in 2021

2 The collateral damage of mismanaged fraud

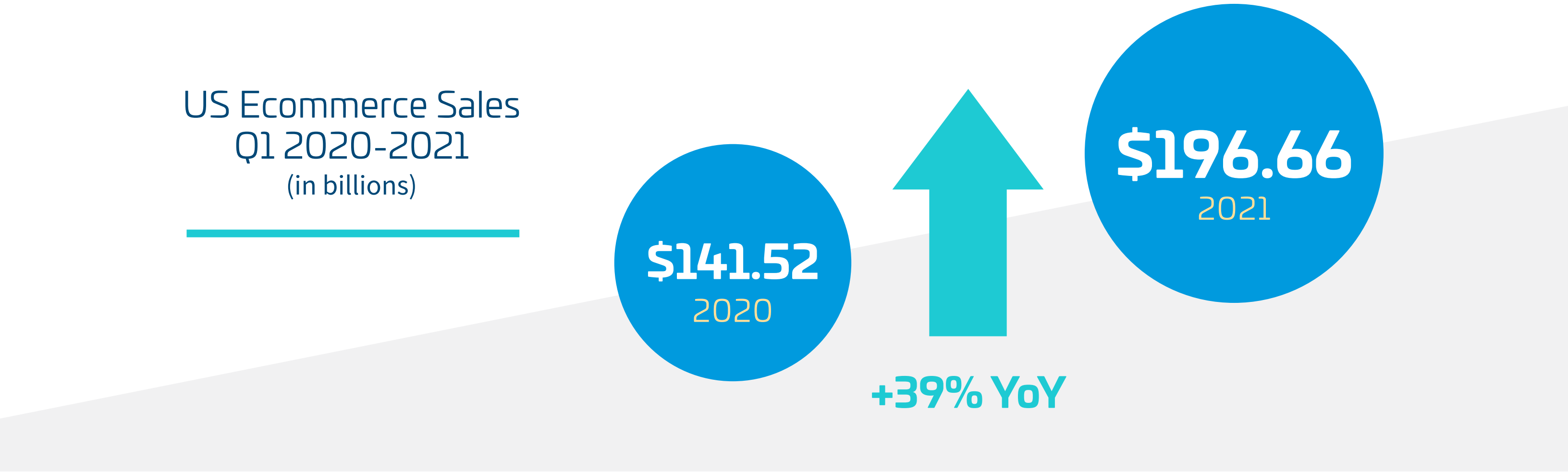
3 How to manage fraud holistically

4 Next steps

1 The Current State of eCommerce

It’s no secret that eCommerce penetration has increased dramatically since early-2020. It’s estimated that consumers spent over **$861 billion** online with U.S. merchants alone in 2020, which is up by a staggering 44% from the prior year.

This unprecedented growth in online spending continued into 2021, with Q1 eCommerce sales in the U.S. reaching **$196.6 billion** – a 39% increase over the prior year.



Source: Digital Commerce 360 analysis of US Department of Commerce data; May 2021

The widespread adoption of the eCommerce channel by traditional brick-and-mortar retailers was a key driver in this spending increase.

Here’s the problem: the sudden growth in online spending has prompted a rise in card-not-present (CNP) fraud. In 2020, CNP fraud cost merchants an **estimated $35.54 billion** globally. That number is only projected to grow as more consumers shift to eCommerce as their primary channel for purchasing products and services.

What are the driving forces behind this increase in fraud?

1. **New purchasing behaviors makes it difficult to identify fraudulent transactions.** Traditional fraud prevention software relies on identifying patterns in purchasing behavior to help spot fraudulent orders. As purchasing behavior fluctuates—as it did quite often throughout the pandemic—it becomes challenging for fraud platforms to quickly adapt and understand this new behavior. For example: Last year, eCommerce brands that sold home office supplies likely experienced a dramatic increase in orders when consumers shifted to working from home. This unexpected change in average order volume presented an opportunity for fraudsters to bypass the typical risk threshold rules that may have been in place several months prior.
2. **Merchants don’t have the proper tools to prevent fraud attacks.** Many eCommerce businesses simply weren’t prepared for the influx in fraud attacks that have occurred in the last year. Merchants that were new to eCommerce may not have had the proper tools to effectively

prevent fraud. Traditional identify verification methods that use physical attributes (IP address, date of birth, social security number) are becoming less effective at accurately identifying fraudulent orders.

3. **The scale and sophistication of fraud attacks is expanding.** The use of botnets and automation is allowing fraudsters to carry out attacks at a much greater scale than ever before. Traditional identify verification methods that use physical attributes (IP address, date of birth, social security number) are becoming less effective at accurately identifying fraudulent orders.

As fraud becomes an increasingly difficult problem to manage for merchants, the costs associated with fighting fraud are also increasing.

2 The Collateral Damage of Mismanaged Fraud

Both the direct and indirect costs associated with fraud are increasing along with the rising number of fraud attacks.

A 2020 report from the Association of Certified Fraud Examiners revealed just how impactful CNP fraud can be on a business's bottom line. The report noted that companies lose roughly 5% of their revenue to fraud each year. This is factoring in chargeback-related expenses, lost inventory, operational costs associated with shipping fraudulent orders, and **false declines**.

5%

Yearly Revenue Lost to Fraud

Lost Inventory

False Declines

Chargeback Expenses

Operational Costs

False declines are undoubtedly the most detrimental result of fraud. Merchants are projected to lose **$443 billion** in false declines by the end of 2021 alone.

Direct fraud loss is a significant component of the total cost of fraud, but we can't overlook the fact that it's also the catalyst for loss in other areas of your business. The indirect cost of fraud may not be as easily measured, but it's just as detrimental to the success of your business.

Consider the following indirect costs that CNP fraud can impose on merchants:

1. **Decreased customer trust.** Falling victim to a fraud attack can erode customer trust and influence the perceived trustworthiness of your brand. In a **recent survey**, 81% of consumers said they would stop engaging with a brand online following a data breach.

2. **Increased operational costs.** Businesses that deal with a high volume of fraudulent transactions often need to employ an in-house fraud team to manually review transactions and ensure that their fraud software is working properly. Additionally, chargeback remediation can put strain on your finance team as it's not always a simple process to undergo.

3. **Damaged customer experience.** If your fraud software interferes with the customer experience of your website, it's very likely that users will switch to a competitor before they purchase from you again. For example, if your website's checkout process involves multiple ID verification steps, this friction will result in customers bouncing from your website before completing their purchase.

4. **Tarnished brand reputation.** If your company has a high fraud rate, you can potentially be flagged as a high-risk vendor by card networks. This will result in higher card processing fees, and in some cases may lead to your business getting blacklisted by a card network.

Many businesses are investing in fraud prevention platforms to protect their revenue. If you're worried about the cost/benefit of paying for these services, check out Vesta's **fraud savings calculator**. This can help you make an informed decision.

Related Resources:

Infographic | The Direct and Indirect Costs of Fraud

Blog | What Are the Costs of Not Having ECommerce Fraud Protection?

Whitepaper | Addressing the False Decline Epidemic

3 How to Manage Fraud Holistically

Businesses need to take a strategic approach to how they manage and prevent fraud. Organizations that move towards a holistic fraud prevention program don't just manage fraud more effectively, but also have a better structure for preventing future attacks.

Understanding your fraud rate will help you manage it effectively.

Here are six key principles that will help to improve your ability to fight fraud:

1. **Understand your fraud and acceptance rates.** Understanding how your fraud rate is measured is the first step in learning how to effectively manage fraud. If you were to accept 100% of the transactions that come through your website – how many of those transactions would be fraudulent? Measuring your fraud and acceptance rates against **industry benchmarks** will help give you a good idea of how your business should be performing.

2. **Implement strategic, not stringent rules during checkout.** Many fraud prevention platforms rely on pre-determined rules that flag orders as fraudulent if they don't meet a specific criteria. For example, orders that are placed with a domestic billing address but an international shipping address might be flagged as fraudulent, even if the order is placed by a legitimate customer. Merchants need to optimize their fraud detection rules based on extensive knowledge of their audience. This is one of the best ways to improve the success rate of future transactions and reduce the likelihood of false declines.

3. **Employ low-friction authentication.** Use biometric and behavioral analytics to reduce friction with authentication and validation during the checkout process. Biometric authentication is less intrusive on the customer experience and is becoming a standard for eCommerce businesses.
4. **Implement return and refund policies that minimize friendly fraud.** Instead of filing a chargeback with their banks, you want your customers to reach out to you and facilitate a refund and return for products that did not meet their expectations. Make sure that your return and refund policies are prominently displayed on all relevant channels such as your website, social media channels, order confirmation emails and receipts.
5. **Integrate machine learning solutions to improve speed and decisioning.** AI and **machine learning** combine to create computer systems and machines that think like us but faster, more reliably… and never need to sleep. For fraud prevention, that means many more sources of data can be analyzed, from more angles, in real-time. Use manual reviews periodically to allow your fraud managers to understand what transactions were automatically accepted, declined, and submitted for further evaluation.
6. **Invest in fraud-related chargeback guarantees.** Investing in fraud-related chargeback guarantees is like investing in insurance policies. The reality is at some point, you will be hit with fraud-related chargebacks. The volume of chargebacks can be higher or lower depending on the season (i.e., peak shopping seasons are often associated with higher chargebacks). Having a chargeback guarantee minimizes the financial loss on your end.

Applying these principles to your fraud management program will help you achieve more impactful results and will lead to significantly reduced fraud losses in the long-term.

The direct benefits you can expect to see from a well-managed fraud program include:

- Higher approval rates, and increased revenue
- Increased customer lifetime value
- Simplified and frictionless customer experience
- A better view and understanding of your target customers

Related Resources:

Whitepaper | The Merchant's Guide to Chargeback Management

Blog | eCommerce Fraud Trends You Need to Know About

4 Next Steps

The true cost of eCommerce fraud is undeniable. As consumers continue to shift toward online shopping as their primary purchasing channel, it's essential that eCommerce businesses have a proper fraud solution to help manage and prevent fraud attacks.

The eCommerce landscape is becoming increasingly competitive, and the customer experience is an important battleground among merchants to win and retain customers. With a fraud solution powered by advanced machined learning technology, you'll be able to keep your customers happy while also stopping fraudulent orders from getting past your authentication barriers.

Vesta is the only instant end-to-end transaction guarantee platform that uses machine learning trained on 25+ years of global data across the world's largest mobile networks and digital merchants. We focus on protecting your revenue from chargebacks and fraud so you can focus on your company's strategic growth. We approve over 97% of transactions and assume 100% of the cost of fraud for what we approve. As a result, Vesta drops the cost of fraud to zero.

If you're interested in learning more about our end-to-end transaction guarantee platform, **schedule a demo** now.

Vesta is a global fintech pioneer in payment and account fraud protection.

If you are concerned that your current fraud prevention tools aren't enough to stop account takeover fraud from occurring, you may consider looking into our Account Protect solution. Contact us today for a free demonstration to learn how we can fortify your defenses eliminate the cost of fraud.

Contact us today and learn how to get our **100 percent** chargeback guarantee.

REQUEST DEMO