



Chargeback Management

The Past, Present, and Future of
Challenging Improper Chargebacks

An Ongoing Need for Chargeback Management

If used as intended, chargebacks are a normal part of the relationship between merchants, payment processors, card issuers, and consumers.

Requesting funds back due to a fraudulent transaction is an important recourse for customers to have, one that makes them more confident in making online purchases. When chargebacks are used improperly then the problem begins. This happens when consumers request their money back due to confusion, buyer's remorse, or an intent to defraud companies and receive free goods. With chargeback rates rising, it is important for companies to make sure they have advanced systems in place to detect these types of misuse and fight back. Failure to curb falsified chargebacks does more than simply take money out of a business's pocket. High rates of upheld chargebacks can bring tougher oversight and penalties from the card schemes and card acquirers, not to mention possibly damaging the company's long-term prospects with card issuers.

Chargeback management has evolved over time.

It is worth reviewing how the current landscape came to be, both to develop an organization's ideal approach for today and to prepare for a future of even greater technology.

The State of Chargebacks

As eCommerce grows, so does chargeback abuse. Misusing chargebacks is becoming more common with online transactions, where a buyer claims that a charge was made fraudulently or services did not meet expectations falsely.

Worldwide chargeback volume is on an upward trajectory and is expected to reach 337 million transactions a year by 2026, with a monetary value of \$15.3 billion.¹

Managing chargebacks has become a costly and time-consuming effort for today's companies. As eCommerce volumes rise, they have been accompanied by an increasing number of people realizing that falsely escalating a charge as "fraud" can result in a quick and likely statement credit. Couple this with the situation when companies fight fraud coded chargebacks, they win less than 20% of the time², and therefore lose out on the revenue and still experience all the operational expenses.

Consumers facing difficult macroeconomic conditions may be tempted to use a falsely coded chargeback to undo a payment when they do not feel capable of going through the accepted channels to receive a refund. These buyers are on the less dangerous end of the spectrum though no less disingenuous. Companies can potentially prevent their actions by creating clearer, user-friendlier return options which allow for the consumer to receive their monies back more easily.

However, many consumers have learned these behaviors and continue to repeat them. Those intentionally using falsely coded chargebacks as a tactic to obtain free goods can cause repeat damage to businesses because of this. Defenses against these types of crimes will need to involve a multi-layered approach by the company. They will need to utilize advanced detection methods to identify the fraud in progress, followed by efficient evidence gathering within the representment process. They may also layer in pre-dispute products to deflect some of the chargebacks coupled with real time alerts allowing them the flexibility to refund true fraud proactively.



Chargebacks' Place in the First-Party Misuse Ecosystem

Understanding falsely coded chargebacks involves looking at the bigger picture of first-party misuse. Once commonly called “friendly fraud,” this is the process of consumers taking advantage of companies’ systems for their own benefit. It is different from more organized and large-scale criminal fraud but can still significantly damage a company’s finances. Misusing chargebacks is one of the primary forms of first-party misuse. Other forms of deliberately attempting to defraud merchants include:



Return policy abuse, in which customers use free returns to “showroom” items they do not intend to buy, or else use products once and then return them for their full value.



Refund fraud, which involves declaring that an item was never delivered and then asking the merchant for reimbursement.

When asked to identify the leading motives for first-party misuse:³

- 58%** of merchants stated that perpetrators were simply attempting to obtain free goods or services;³
- 38%** said people were trying to return goods beyond the allowed time frame;³
- 29%** cited simple buyer’s remorse.³

Other, potentially more benign, reasons for chargeback activity include confusion about the way charges appear on bank statements (47%) or receiving goods and services that were not up to the expected quality (37%).⁴

Some kinds of first-party misuse can be counteracted through policy changes. For instance, if consumers are consistently confused by the way charges appear on their bills, companies can adjust their billing descriptors by working closely with their payment processor. In cases where return policy confusion is the key issue, they can try to clarify the policy further and ensure customer service can clearly articulate why or why not something is eligible to be returned.

Battling improperly coded chargebacks caused by simple buyer’s remorse or intent to defraud, however, calls for a dedicated approach to detecting and challenging these disputes. The methods companies used have developed and evolved over the years.

The Past:

The Development of Chargeback Management Methods

Challenging a disputed transaction to prevent or reverse a chargeback means assessing the evidence to determine whether the customer has acted improperly. In short, this is the process of verifying that when a consumer claims fraud as a reason for reversing a credit card transaction, that fraud has really occurred.

Historically, the work going into this representment process has been heavily manual. The general process involves teams of employees checking customer records and determining the facts of each case individually.

Employees collate these details into a document and submit it to the card issuer, which judges whether the case has merit. Accuracy is at a premium in these cases. Companies must be sure the disputes they are challenging are truly improperly labeled.

False positives are so damaging to consumer relations that they are also called “customer insults.” The rate of these accusations ranges from 2-10%.⁵

The flaws of this system largely revolve around the difficulties of scale. Manually assembling a representment document for every challenge can be time-consuming and labor-intensive, demanding attention from many employees. In addition, the people building the representment documents will inevitably approach what they include and how they explain why it is not fraud differently. This is true even if they are at the same company which increases the challenge for the Issuer being able to understand the merchant’s responses. Though this process is sustainable on a small scale, the current volume of hundreds of millions of chargebacks requested every year has strained the ecosystem to its limit.

While this process is limited by its manual nature, it is fundamentally sound. Efforts to evolve the process have largely revolved around adding more automated elements rather than fundamentally changing the way merchants contest chargebacks. Companies seeking to better use their employees’ time and effort can do so by using chargeback management platforms that help to automate some or all the representments.

Evidence of an improperly requested fraud-coded chargeback can include:

- ✓ Photographic evidence that goods were delivered.
- ✓ Details of the transaction in question (device used, buyer location, and more).
- ✓ Historic patterns of activity between the customer and the company.

The Present:

Compelling Evidence and Automation

Recent years have brought some developments in the relationship between merchants and credit card issuers, collectively designed to make chargeback management a more streamlined process. One key concept is the introduction of Compelling Evidence rules.

Compelling Evidence programs are sets of criteria that allow companies to provide specific information about the relationship the consumer has with the merchant or the service's recipient as well as how the service was fulfilled. Instead of submitting only visual evidence for the representment process, merchants can instead provide data evidence, visual evidence, or in some cases both types showing how customers have interacted with the business, signifying that a charge wasn't the product of fraud.

Most recently, Visa's Compelling Evidence 3.0 Framework is designed to allow merchants to challenge transactions tagged with "dispute condition 10.4," indicating Card-Not-Present (CNP) fraud.

Merchants who provide this evidence through digital services such as the Order Insight and Consumer Clarity solutions can connect with the card issuer using a real-time data exchange. Of course, a merchant can also provide this information as part of the representment process as well.

While Compelling Evidence rules provide a powerful way to exchange data and have disputes resolved, they are not universally integrated by issuers and acquirers at this stage. With the technological infrastructure still lacking in many cases, merchants today largely rely on the standard representment methods involving the manual assembly of evidence documents verse the more data driven process CE3.0 was meant to drive.

Fortunately, there are ways to make conventional dispute challenges more efficient through the application of automation. Chargeback management platforms that use machine learning and related algorithmic methods to assess transaction data, can either look to automate the process or at a minimum help employees make quick and accurate decisions about which chargebacks to challenge.

To have their cases upheld, those merchants must share evidence of two past transactions with the same customer that:

- ✓ Have no fraud reports or disputes.⁶
- ✓ Occurred between 120 and 365 days before the dispute.⁶
- ✓ Match two or more personally identifying data elements with the disputed transaction such as IP Address and Device Fingerprint.⁶

With data-based insights allowing them to act more efficiently, these teams can accomplish more with the same level of staffing.

This is an essential competency as the volume of chargeback claims mounts. And it is one that can bridge the gap while waiting for wholly digital methods to become more widely available.

The Future: Leveraging The Power of AI

The next steps for organizations' chargeback management efforts will include the addition of increasingly advanced capabilities to smooth out the representment process. Advanced Machine Learning algorithms and the advancement of Artificial Intelligence, some of the hottest trends in technology development, have a real role to play here.

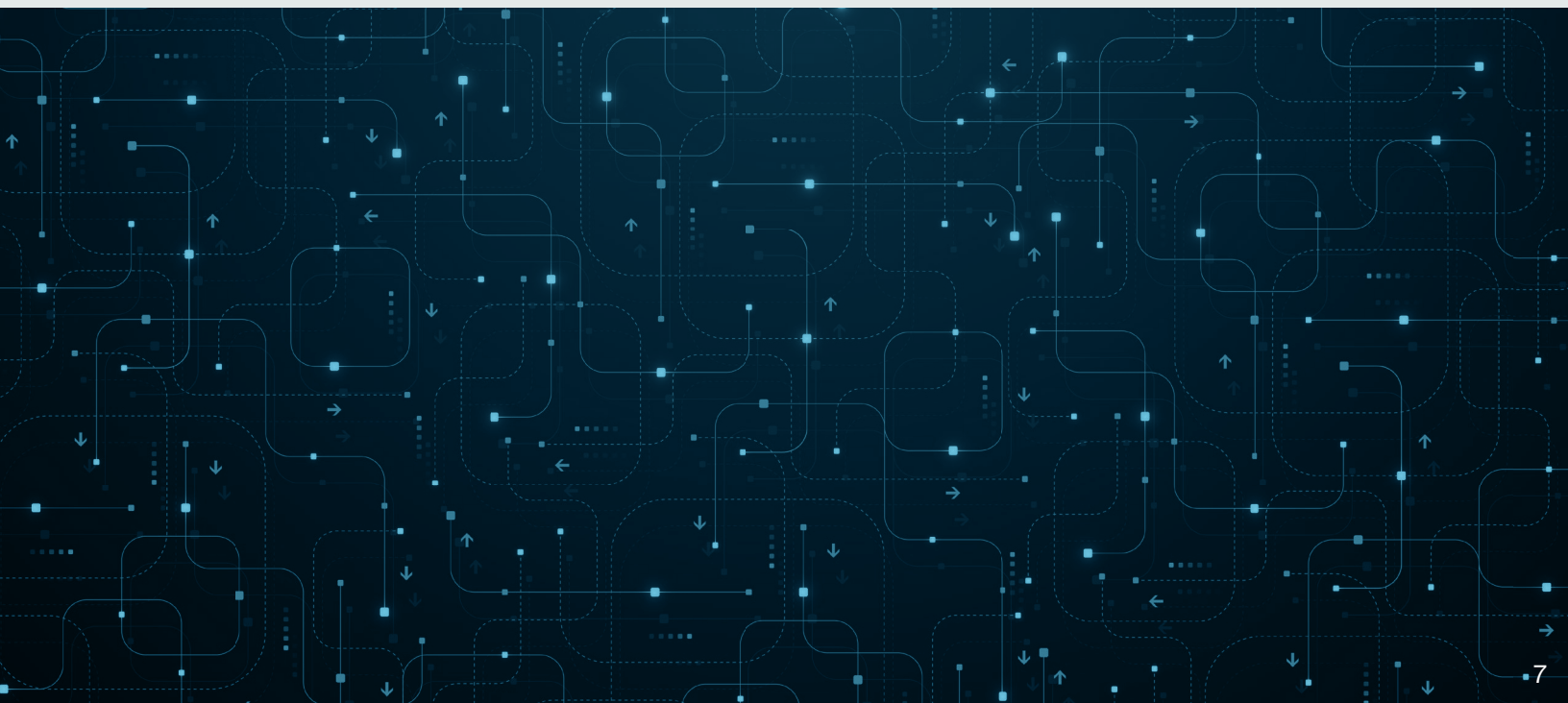
Next-generation chargeback management workflows can incorporate more and more data to make better decisions about what is fraud versus first-party misuse to ensure a merchant's focus is on items which are winnable.

You also have efficiency-building Artificial Intelligence tools that can assemble evidence for review by card providers. As with other office tasks where AI-powered tools and increased automation can lead to faster, more efficient everyday activities, workers will potentially be able to produce more representments more quickly, increasing their individual productivity.

While using Artificial Intelligence to pull the required information and assemble it into human legible documents is a potential next step for chargeback management, there is room for even further digitization. Systems that can seamlessly exchange data between merchants, acquirers, payment networks, and credit card issuers represent a viable endpoint for chargeback challenges.

Under such a system, the need for human intervention would decrease drastically. This in turn, helps resolve the scale-based issues that are holding merchants back as they attempt to compete with the large volume of chargebacks coming in today.

While these features mostly remain in development, there are powerful chargeback management offerings on the market today pushing these boundaries. By adopting the existing technology and methods, organizations can battle first-party misuse now and lay the groundwork for next generation methods.



What To Look for in a Chargeback Management System

A merchant's chosen technology platform can determine how successfully it manages to keep up with chargeback volumes. With an effective digital system, it is possible to make challenges more accurate and assemble the necessary evidence quickly. Without one, companies may find themselves overwhelmed with the sheer volume of disputes and chargebacks coming in.

The key features of such a system include:

- ✓ The ability to automate the representment process is key to being able to scale, drive consistency, and ensure you minimize expenses while maximizing revenue recovery. However, sometimes you may need employees to enhance the process and strong automation can support them by assembling representment files quickly and efficiently, allowing each employee to accomplish more in each day.
- ✓ Human-led design and configuration to align the platform with the company's unique needs based on its scale, industry, region, typical customer profile, and more factors. This ensures the flexibility needed to handle a company's exception processes which are meant to ensure a good customer experience and minimize revenue leakage.
- ✓ Another core piece is advanced data analytics tools, powered by methods such as machine learning, to read signals more quickly and accurately, and determine which challenges are likely to be fraudulent. This ensures you minimize customer insults by reducing an analyst accidentally fighting true fraud and ensuring the focus stays on what is winnable and generates value for a company.
- ✓ Another important aspect of data analytics is ensuring the platform offers a robust set of Key Performance Indicators (KPIs) dashboards and reports. These tools provide visibility into business performance, particularly in relation to chargebacks. Reporting should also offer insights into analyst productivity, such as throughput and success rates, so you can effectively measure performance and support underperforming team members. Finally, while no reporting tool can deliver every report imaginable, the platform should allow data to be easily extracted. This enables integration with your existing business intelligence tools or, at the very least, supports the creation of custom reports tailored to your needs.

A strong collaborative bond between a merchant and its chargeback management provider is essential for staying ahead of evolving trends in first-party misuse. By working closely together, businesses can quickly adapt to emerging patterns and integrate advanced features as they become available, helping to proactively combat malicious and fraudulent chargebacks. Just as important is choosing a partner that actively seeks and incorporates customer feedback as part of their everyday approach to collaboration.



Providers who prioritize on going dialogue and input from their clients are better positioned to align their roadmap with real world needs, ensuring the solution evolves in step with the challenges merchants face.

Companies Can Not Afford To Neglect Chargebacks

With hundreds of millions of chargeback incidents occurring annually and billions of dollars lost, effective chargeback management is essential for every merchant. As eCommerce continues to dominate the globe, organizations must treat all forms of card-not-present fraud as critical threats to their bottom line and take proactive steps to mitigate them.

Today's cutting-edge chargeback management and prevention methods point the way to an even more automated future of AI-enabled efficiencies and, eventually, digital contact between merchants and card providers.

Implementing a chargeback management platform with the aid of a trusted and collaborative partner organization is an essential step in the overall fight against first-party misuse. While the money lost to first-party misuse is just a portion of overall fraud losses and a fraction of the overall market for online commerce, its impact on a single company can be significant.

Sources:

1. <https://464903.fs1.hubspotusercontent-na1.net/hubfs/464903/2023%20Chargeback%20Outlook%20Report%20-%20FINAL.pdf>
2. https://info.merchantriskcouncil.org/hubfs/Reports/Fraud%20Reports/2024_Global_Payments_and_Fraud_Report.pdf
3. https://info.merchantriskcouncil.org/hubfs/Reports/Fraud%20Reports/2024_Global_Payments_and_Fraud_Report.pdf
4. https://info.merchantriskcouncil.org/hubfs/Reports/Fraud%20Reports/2024_Global_Payments_and_Fraud_Report.pdf
5. https://info.merchantriskcouncil.org/hubfs/Reports/Fraud%20Reports/2024_Global_Payments_and_Fraud_Report.pdf
6. <https://usa.visa.com/content/dam/VCOM/regional/na/us/support/legal/documents/compelling-evidence-3.0-merchantreadiness-mar2023.pdf>

Contact Accertify
to learn more about how
to manage chargebacks
effectively and learn to
move at the speed of right.