

# Quantifying the challenge of friendly fraud



## Your post-purchase strategy for the future

- The role of data
- Misconceptions of the effectiveness of In-house solutions
- Data storage
- Upgrading data collections system to optimize your data
- Audit and optimize



# Contents

**Intro** **3**

**Quantifying the challenge of friendly fraud** **4**

**The role of data** **8**

**Misconceptions of the effectiveness of In-house solutions** **9**

**Data storage** **11**

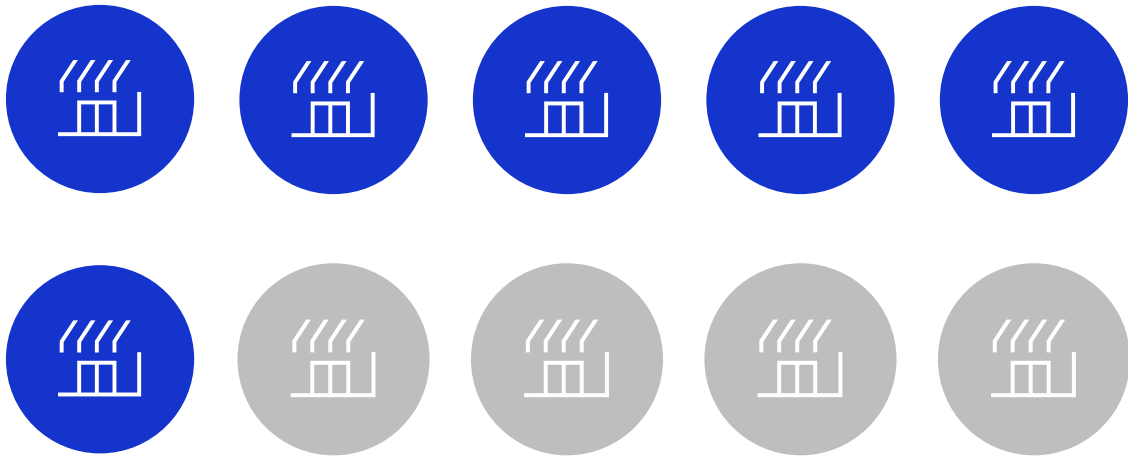
**Upgrading data collections system to optimize your data** **13**

**Audit and optimize** **14**

**Key takeaways** **15**

**About MFJ** **16**

**About Verifi** **17**



## More than six in 10 merchants cite an increase in first-party-misuse (FPM) over the past year<sup>1</sup>.

Of that cohort, half believe that incidences of friendly fraud increased by 25%<sup>1</sup>. A wave of card network dispute rule changes, that started in April 2023, allow merchants to stop first-party fraud through the submission of qualified transaction data. As the use of data becomes increasingly pre-eminent in the post-purchase ecosystem, merchants will benefit from leveraging data.

What does this mean for merchants and what their post-purchase strategy should look like for the future? Let's explore the growing role of data and how it presents a novel dispute strategy to the problem of friendly fraud.

<sup>1</sup>[Verifi's 2024 Global Fraud & Payments Report](#)

## Quantifying the challenge of friendly fraud

How did data become instrumental as a friendly fraud defense? First-party-misuse (FPM), by its nature, is hard to measure and very unpredictable. Friendly fraud (and in the context of chargebacks, human intention) is complex and ambiguous. But data can help manage the various aspects of FPM:



### **Time delay management:**

Friendly fraud often happens long after the purchase. That makes it hard to track and, monitor even more so if you deal with a high volume of disputes. Human memory can fade, inventory overturns rapidly, and evidence may disappear; but first-party-misuse can be successfully identified with clean and accessible data. The storage and submission of qualified data to card brands can block the eligibility of disputes.



## Understanding unclear indicators:

First-party misuse often displays no immediate signs of illicit activity. For example, a priority customer might file a surprise chargeback when they do not receive their product. Little do they know that a family member accepted the shipment on their behalf a week earlier. Once they file the honest dispute, fraud occurs by accident.



But with high-quality data analysis, merchants can catch fraudulent disputes using data that proves delivery and provides clear indicators of an established pre-existing relationship between the cardholder and the merchant.

### **Bridging the gap on confusing descriptors:**

Cardholders may not immediately recognize a transaction by descriptor. Think of a video gamer making a purchase at an in-game store. Buyers know the name of the game enhancement purchase; however they may not know the name of the game company that shows up as the descriptor on a credit card statement.



If the merchant provides additional purchase data to the issuer, cardholders are more easily able to identify the purchase at the point of inquiry, preventing the cardholder from proceeding with a dispute.



## Seasonality:

Chargeback volumes peak with seasonality. Different verticals experience high chargeback volumes during different seasons, often sparked by the close of the holiday season. Data storage and analysis can help merchants anticipate when they may experience a surge in disputes. Third party solutions can more effectively help manage sudden high volumes without disruption to the business.

**2/3**

of merchants with annual revenues greater than \$1B use in-house dispute management methods rather than third-party services<sup>2</sup>

resulting in

**16-34%**

greater revenue losses than merchants who utilize solely third-party platforms to manage disputes<sup>2</sup>

## Economy:

In harder economic times, consumers have been known to file more chargebacks. Storing the appropriate data can help merchants protect against cardholders who may file disputes as a means of recouping funds when they are struggling financially.

## Complexity of data requirements:

Each card networks has their own unique data requirements. For merchants who don't have the resources, the different needs can be a barrier to entry, but third-party solutions can help streamline data storage and accessibility for seamless compelling evidence qualified data submission.

<sup>2</sup>[PYMNTS.com Dispute Prevention Solutions: Third Party Tools Limit Dispute Related Losses](#)

## The role of data

Merchants can share the necessary data to avoid illegitimate disputes either prior to the initiation of a dispute, or after a dispute has been filed. When an inquiry is raised, real-time enhanced data sharing solutions relay cardholders' past purchase information instantaneously from the merchant back to card networks in the pre-dispute phase – stopping or “deflecting” the dispute from ever being filed and being factored into the merchant's dispute ratio.



Alternatively, merchants can leverage the new compelling evidence remedy in the post-dispute phase, by manually sharing data as part of a pre-arbitration response; however, if the data sharing occurs after the dispute is recorded, the dispute will still be factored into the merchant's dispute ratio.



## Misconceptions of the effectiveness of in-house solutions

There is a breakdown between expectations and reality when it comes to dispute prevention. Studies show that merchants overrate the effectiveness of their in-house dispute strategies, when in fact, third party services are more effective than merchant propriety systems.

### Revenue Loss

1%

Merchants using  
third-party tools<sup>2</sup>

2.9%

Merchants using in-house  
proprietary tools<sup>2</sup>

Merchants using only third-party tools only lost 1% of their card payment revenue in the prior 12 months. By contrast merchants using only in-house propriety tools lost 2.9% of revenue<sup>2</sup>. Why are third party services more effective than in-house solutions that theoretically have the best insight on the situation?

<sup>2</sup>[PYMNTS.com Dispute Prevention Solutions: Third Party Tools Limit Dispute Related Losses](#)

Card networks have created compelling evidence requirements that allow for the submission of specific data points to guarantee the dismissal of card-not-present fraud disputes; but for other dispute reason codes it can be tough for merchants to know which data is most relevant to submit as compelling evidence.

**20%**

Merchants struggle to win fraud-coded disputes<sup>2</sup>

**35%**

Rate their measures as extremely effective against FPM<sup>2</sup>

### **Choosing the right data:**

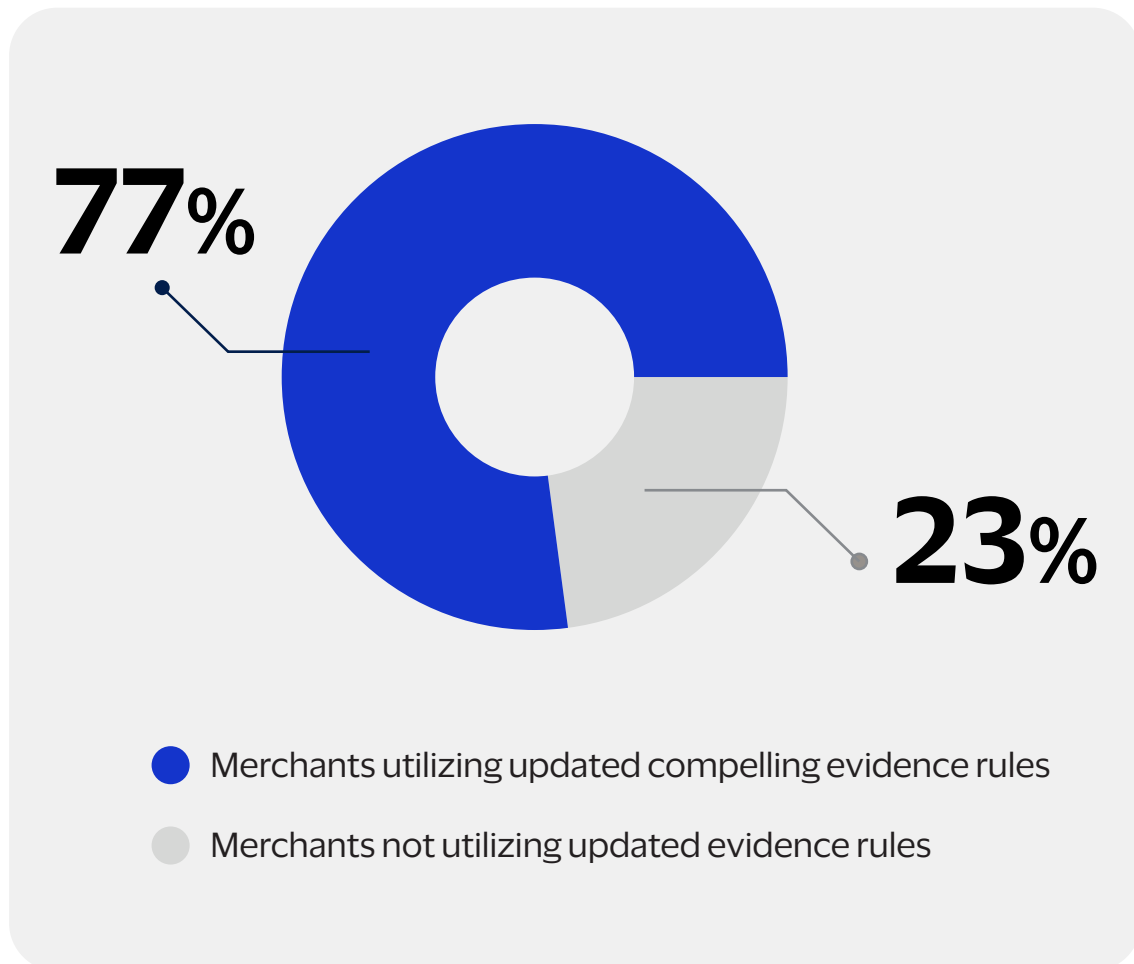
Each reason code and card brand have very specific and evolving data requirements. To win cases you need proof. And that requires a volume of data. Unfortunately 20% of merchants report that they struggle to win fraud-coded disputes with in-house dispute management. And less than 35% of merchants rate their filing and fighting measures as “extremely effective” in countering FPM. In reality, data provides the comprehensive proof needed to refute false claims. With a focus solely on data and disputes rather than the entire merchant business, third-party solutions are up to date on evolving card brand compelling evidence data and submission regulations.

<sup>2</sup>[PYMNTS.com Dispute Prevention Solutions: Third Party Tools Limit Dispute Related Losses](#)

## Data storage

### Looking to the future: How merchants can prepare

Data offers new and exciting opportunities for dispute prevention. In the past year, 8 in 10 merchants report the successful use of data submission to leverage the changes to compelling evidence requirements. Over three-quarters (77%)<sup>1</sup> of merchants have utilized card networks' updated compelling evidence rules to block or reverse first-party misuse disputes.



Those who do not have proper data management will be ill equipped for the new payment environment.

<sup>1</sup>[Verifi's 2024 Global Fraud & Payments Report](#)

## So how can a merchant prepare?

The accessibility of relevant data is key. First-party misuse can occur in a matter of seconds, so response time must keep pace. Merchants will need to work towards optimizing the search of data to eliminate any delay between the initiation of a first-party misuse dispute and their response time with the evidence to prove legitimate past purchase behavior.



Merchants who utilize multiple systems to store relevant data elements need to critically evaluate their database design, data storage, and searching mechanisms to ensure they can respond in real-time to effectively leverage the automatic deflection remedy during pre-dispute processing.



## Upgrading data collections system to optimize your data

Now is the time for merchants to invest in systems that collect the necessary depth of data. Systems may include:

- **Centralized data repositories:**  
Data warehouses, data lakes, relational databases, etc
- **Transaction data analysis tools:**  
Enhanced eCommerce, host dashboard tools. Power BI tools, Customer Relationship Management (CRM) tools, etc
- **Evidence documentation:**  
Digital receipts, transaction logs, order management, delivery confirmations, document management systems, etc
- **Authentication tools:**  
Biometrics, Multi-Factor Authentication (MFA), Token-based authentication, Single Sign On (SSO), etc
- **Customer verification:**  
Card Value Verification (CVV), Address Verification Systems (AVS), personal payment info, contact info, etc
- **Adaptive authentication:**  
Geolocation data, IP addresses, device IDs, login behavior, network data, contextual data. etc
- **Data management and security:**  
Encryption, backups, access controls, data masking, HTTPS, PCI-DSS compliance, etc

## Audit and optimize

Critically evaluate your database design, data storage, and searching mechanisms. You need to be able to relay pertinent cardholder information to card issuers and other services in the current fast-paced landscape.



That means accessibility holds a premium, as FPM can occur in seconds. Data automation also takes on greater importance in improving business responses to friendly fraud. Optimize your data management via:

- **Data integration tools:**  
Data flow, data accessibility
- **Data cleansing:**  
Deduplication, completed data sets, correct formatting
- **Data governance:**  
Data quality and compliance
- **Business intelligence:**  
Analyze and improve
- **Auditing tools:**  
Review models and streamline performance)

## Key takeaways

The prevalence of first-party misuse highlights a critical need for effective prevention strategies. Upon closer examination, we can see four critical takeaways as merchants fight the variable nature of friendly fraud:

- **Data offers a fundamental tool in the fight against first party misuse:**  
Compared to static tools, data (and novel analysis solutions) can effectively detect and limit friendly fraud.
- **Key players recognized this potential and updated:**  
Due to the growing utility of data the industry shifted into a datacentric environment (e.g. Visa Compelling Evidence 3.0).
- **Third-party solutions will be integral in the adjustment:**  
To bridge the resource gap, merchants have turned to thirdparty services to help capture the benefits of data.
- **A data-centric landscape impacts all merchants:**  
The landscape shift necessitates merchants to optimize their data and analysis practices. Those who fail to modernize may fall into increasing technical debt.

In summary, data is increasingly integral in combating first-party misuse. Embracing advanced technologies and data-driven strategies will be essential in navigating the complexities of modern fraud prevention.

**“If everyone is moving forward together,  
success takes care of itself”**

**Henry Ford**

## About Merchant Fraud Journal



**Merchant Fraud Journal** is an independent and unbiased publication dedicated to empowering online sellers to greatly reduce the impact of eCommerce fraud on their businesses. Its core mission is to break the silos surrounding merchants' internal fraud prevention processes by bringing together industry professionals to share their knowledge with one another.

Unfortunately, the business process knowledge needed for online sellers to greatly reduce the impact of eCommerce fraud is scarcely available right now. There is no single forum and resource where merchants, payment professionals, and other industry professionals could go to get educated on the myriad of challenges they face.

We seek to fill that gap by being a resource that collects insight from industry thought leaders and fraud prevention tool experts on topics such as chargebacks, false positive declines, account takeover fraud, friendly fraud, data breaches and more. Our goal is to help honest businesses quickly understand their security options and take action, so they can get back to focusing on their core business activities.



## About Verifi

VERIFI  
A Visa Solution

VISA Acceptance  
Solutions


**Verifi, A Visa Solution**, is a leading provider of next generation post-purchase solutions that streamline the dispute process and improve the customer experience.


Available for all major card brands, Verifi solutions help merchants globally to prevent and resolve disputes by sharing compelling evidence, data transparency and merchant-initiated or rules-based refunding. Verifi equips merchants, issuers and acquirers to reduce financial loss, create operational efficiencies, and remove unnecessary fraud and first-party misuse disputes from the payment ecosystem.





### Contact Merchant Fraud Journal

Editor In Chief - Bradley Chalupski  
Bradley@merchantfraudjournal.com

 290 Caldari Road,  
Concord, Ontario L4K 4J4  
Canada

 hello@merchantfraudjournal.com

 www.merchantfraudjournal.com

 1-(888) 225-2909



### Learn more.

www.Verifi.com | info@verifi.com