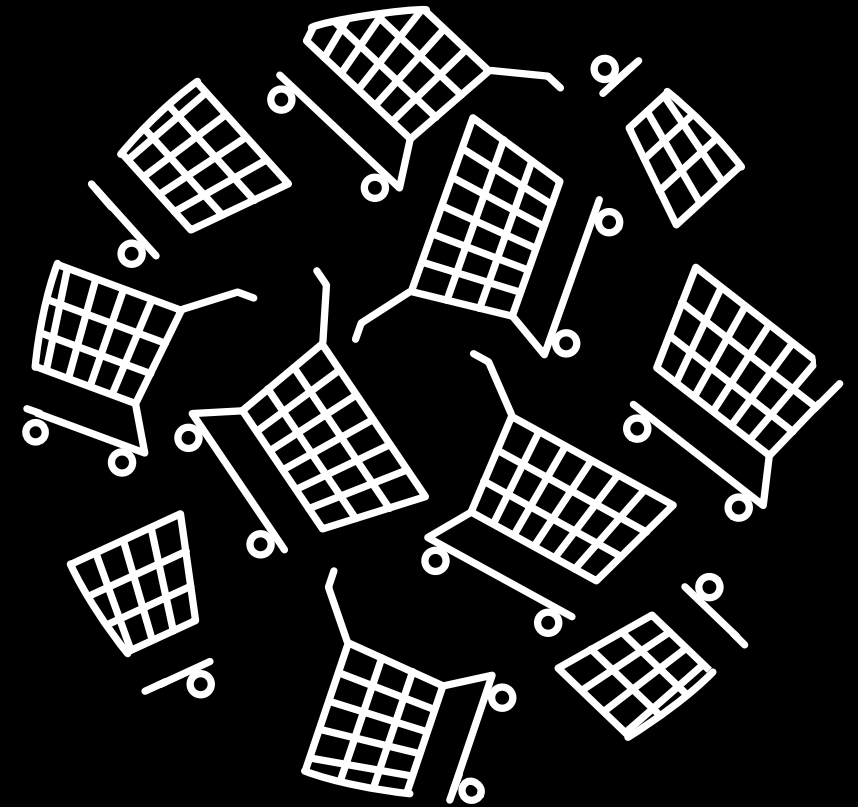# Optimizing eCommerce Payments

Optimizing Payments for e-Commerce Merchants while
Reducing Fraud Risk

March 2024

Deloitte. X riskified

What to expect ?

Deloitte. X ✓ **riskified**

Setting the Context

eCommerce provides exceptional opportunities for revenue and growth by continuously opening doorways to new products, services and customer segments for many merchants. Globally, eCommerce is projected to rise over 40% from $6 trillion in 2022 to over $8.5 trillion in 2026, and within Canada, growth in eCommerce is expected to jump from $97 billion in 2022 to $144 billion in 2026[1].

As this industry continues to expand exponentially, the dynamic landscape driven by fierce competition has created novel challenges that all merchants must overcome to drive success. These challenges range from enhancing the customer experience, gaining customer loyalty, managing data privacy, logistics, risk management, to managing omnichannel payments. This has led to merchants launching initiatives such as re-designing loyalty programs, investing in reducing customer friction, and most importantly focusing on payment optimization in order to remain competitive.

From a payment's perspective, several stakeholders must come together and work cohesively to deliver a seamless experience for the customer – which is easier in theory than in practice. On an average, merchants in North America rely on roughly 3.5 payment gateways/processors and 2.9 acquiring banks to process their payments[2]. This means compounded requirements for merchants to follow, increasing the difficulty of passing risk assessments. There is also an increased risk of fraudsters taking advantage of digital payments as the risk has increased over 80% from 2019 to 2022[3]. Therefore, to optimize eCommerce revenue, a merchant must consider both enhancing payment processes while managing fraud risk.

Optimizing eCommerce revenue requires a dynamic approach to customize the payment journey according to the expected fraud risk. An array of new fraud management solutions are available in the market to help eCommerce merchants tackle fraud. However, the traditional outlook towards fraud solutions as a 'one size fits all' solution limits how they can be applied by different merchants and mitigate fraud risk while maximizing revenue through payments optimization.
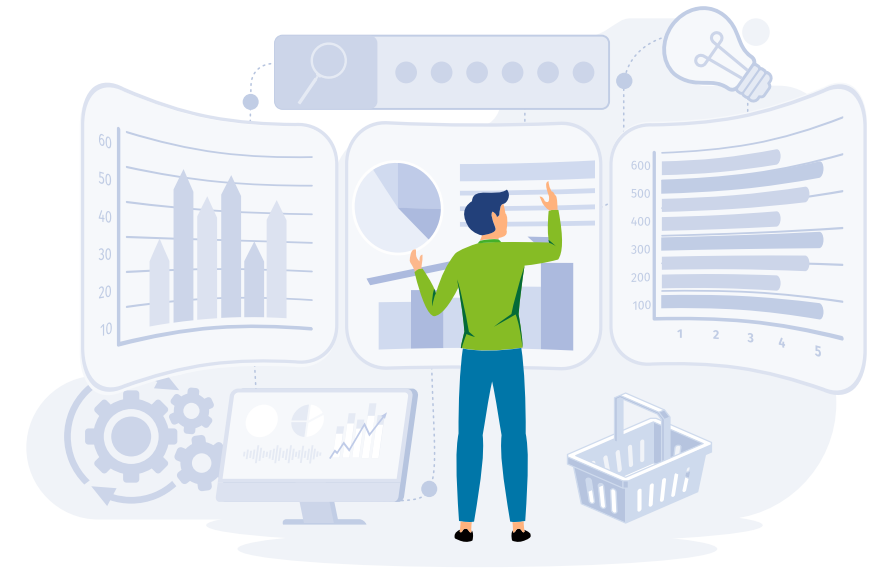
1 Worldpay, Global Payments Report, 8th edition
2 Merchant Research Council, 2023 Global eCommerce Payments and Fraud Report, p. 12, 2023
3 TransUnion, TransUnion 2023 State of Omnichannel Fraud Report, 2023

# Market Trends and Challenges: Why Optimize Payments and Reducing Fraud Risk?

Global industry trends indicate a growing need to **optimize payment processes**, reduce their impact on revenue and customer experience, and **simultaneously manage fraud management costs**

**5.5% of Business revenue is lost to false declines** [1]

5.5%
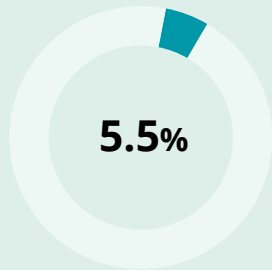
With the global eCommerce market expected to total $8.3 trillion in 2025[2], this translates to around **$457 billion in losses due to false declines**

62% of Consumers will not continue buying from a merchant after experiencing a false decline [3]

62%
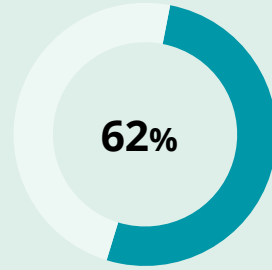
Aside from losing a sale, this can sometimes end the customer relationship, causing merchants to **lose out on customer lifetime value** [3]

10% of eCommerce revenue is spent to manage payment fraud per survey across 440 merchants [4]

10%
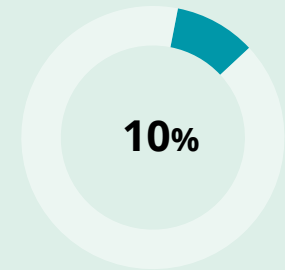
Some merchants are using intelligent payment routing or machine learning to **fine-tune fraud management to optimize payment** authorization rate indicating rising concerns
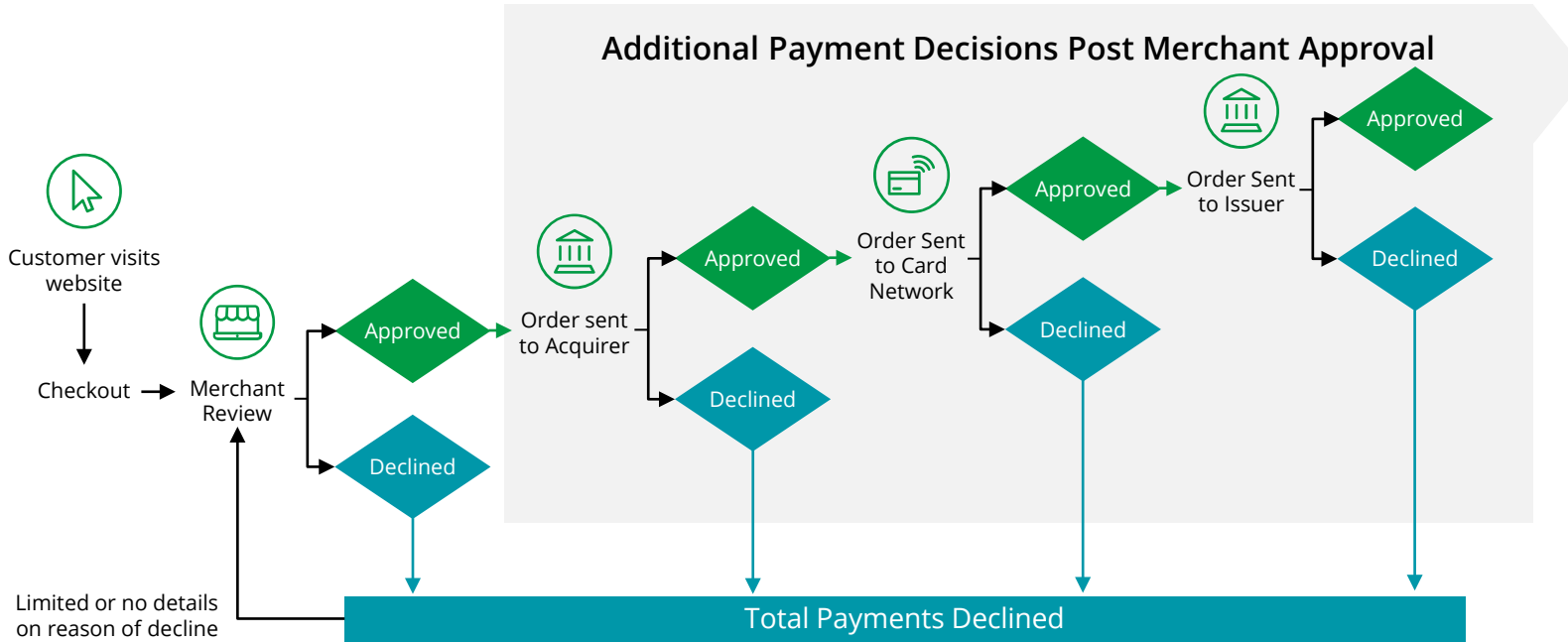
1 Payment Declines in eCommerce | Riskified Blog
2 Global e-commerce Market Projected to Grow 55 Percent by 2025, FIS Study Finds
3 Team, IR. "How Declined Payments Affect Your Business." IR. How Declined Payments Affect Your Business, 2023
4 Merchant Research Council, 2023 Global eCommerce Payments and Fraud Report, p. 14,17, 2023

Deloitte. X ✔ riskified

Payments Journey from an eCommerce Merchant's Lens

Additional Payment Decisions Post Merchant Approval

Customer visits website → Checkout → Merchant Review

Approved → Order sent to Acquirer
Declined

Approved → Order Sent to Card Network
Declined

Approved → Order Sent to Issuer
Declined

Approved
Declined

Limited or no details on reason of decline

Total Payments Declined

How does this "Black Box" impact you?

eCommerce Merchants typically do not have a full view into the end-to-end payment journey. Other entities involved in the payment process, including payment processors, card networks, and issuers, uses their own fraud decisioning solutions to manage their respective liability, which may not be passed back to merchants. Research shows that 50% of merchants surveyed in 2022 reported that they do not receive response codes from FIs on failed payments.

The payment strategy adopted by Merchants can influence the treatment of transactions by other entities along the payment journey. For example, a Merchant focused on maximizing revenue and approving most transactions by lowering their thresholds may be scrutinized and flagged as high-risk by the payment processors/issuers downstream.

Even a small decrease in approval rates due to additional downstream scrutiny can have a considerable impact on the overall revenue.

Challenge in Maximizing Revenue while Managing Fraud Risk

Merchants need to combine their internal payment approval strategy with the impact and understanding of the end-to-end payment journey to find the right balance that optimizes overall revenue while effectively managing fraud.

Focus on Maximizing Revenue

Increases the risk associated with fraudulent transactions and being flagged as high-risk

?
Your organization

- Approve majority payments to avoid instances of false declines
- Less stringent fraud/risk controls

- Tight controls to avoid liability & losses across fraud, waste, and abuse
- High number of false declines

Focus on Minimizing Risk

Increases the risk associated with customer experience and impact on overall revenue

Defining The Payments Optimization Approach That Works For You

Deloitte Digital Payment Approval Optimization Framework and Approach for eCommerce can help merchants determine a balanced solution to most effectively optimize payments.

Digital Payment Approval Optimization Framework

Each lever helps inform the strategic approach to payments optimization on a case-by-case basis. Different considerations support merchants in identifying the unique target state between revenue maximization and fraud risk mitigation.

Geographic Location
Different regions or areas of operation for the merchant may pose different levels and types of exposure, depending on size of the regional business, payment ecosystem, and leading fraud threats.

Brand Architecture
Different sub-brands within an organization or different product categories could require a custom solution to tackle risks depending on customer base, product/service type, product/service value, etc.

Payment Channels
Channels used by merchants for transactions, ranging from in-person, digital, to omnichannel and determining payment type used could inform the approach to select payment decisioning vendors/solutions.

Additional considerations offer supplementary support in considering tailored solution options:

ORGANIZATIONAL FACTORS

Merchant Size: Consider different capabilities relevant to large vs. mid-sized vs. small businesses. E.g., larger merchants with multiple banners may require more complex payment strategy and/or fraud solutions.

Product Type: Consider the nature of product offered by the merchant. E.g., high dollar value products require more stringent payments review process.

Payment Volume & Frequency: Consider the number of transactions handled by a merchant over a period of time. E.g., payment volumes may impact vendor subscription charges and infrastructure requirements

Payment Acquirers: Evaluate the payment acquirers leveraged across all channels to optimize authorization rates and decrease fraud based on transaction type using Decision-as-a-Service (DaaS) such as Riskified

SOLUTION OPTIONS

In-House Fraud Capabilities: Build a custom fraud solution in-house that addresses organizational requirements, which is preferable when capabilities required are unique to the organization

External third-party fraud solutions: Purchase custom off-the-shelf external third-party solutions that offer ready-to-use tools and capabilities or Decision-as-a-Service (DaaS) with approval rate guarantee and liability outsourcing such as Riskified AI Platform

Usage of Network Solutions: Use smart routing tools for payments through 3D Secure based on processing location and leverage 3DS exceptions strategy for optimal approval rates and avoid friction or false declines by network solutions

An Illustrative View Of Optimized Payments Flow

Deloitte's Digital Payment Approval Optimization Framework guides in the identification of a solution targeted to the merchant's unique requirements, by leveraging the framework's considerations.

LEVERS — **PAYMENT FLOW APPROACH**

REGION #1 — BRAND A — PYMT CH. 1 / PYMT CH. 2 / PYMT CH. 3
- Traditional Fraud Review → Payment Approved
- Traditional Fraud Review → Requires Challenge → 3D Secure (3DS) → Approved / Declined
- Traditional Fraud Review → Payment Declined → Decision-as-a-Service (DaaS) → Approved / Declined

Net-new benefit due to approval rate optimization i.e., increase revenue while minimizing cost (fraud losses & 3DS/DaaS expense)

REGION #2 — BRAND A — PYMT CH. 1 / PYMT CH. 2
- Decision-as-a-Service → Payment Approved / Payment Declined

BRAND B — PYMT CH. 1
- Traditional Fraud Review → ... → ... → ...

Legend:
- Existing Payment Process
- New Payment Processes
- Net-New Approval

Approach is **determined by framework levers** such as:
- Geographic Location
- Brand Architecture
- Payment Channels

Complexity and types of solution is determined by framework factors such as:
- Merchant Size
- Product Type
- Payment Volume & Frequency
- Payment Acquirers

These factors inform **the type of solution** such as:
- In-House Build
- Third-Party Solution
- Network Solution

What can you do?

To optimize payments and revenue while reducing fraud, merchants should be open to:

1. **Implementing non-traditional payment approval strategies**

2. **Investing in minimizing fraud and leakages** that may occur after implementing alternative payment channel/s

Doing so will not only maximize benefits in terms of growth of revenue using a tailored approach but also result in efficient management of current and emerging fraud risks.

The most challenging step towards implementing a non-traditional strategy for payments optimization is to identify where to start.

We can help you grow ahead of the curve by applying Deloitte's Digital Payment Approval Optimization Framework and Riskified's AI-powered Fraud and Risk Intelligence Platform.

The Way Forward

A three-step approach will help your organization identify a right-sized payment optimization solution.

1   Involve the Key Relevant Stakeholders

- Identify and involve key relevant stakeholders across the organization to successfully inform and identify the target state payments strategy, including but not limited to, e-Commerce, Digital Solutions, Payments, Fraud, and Finance functions.

Expected Outcomes

- One enterprise payment approval strategy across multiple organizational functions

2   Benchmark Using Industry Intelligence

- Conduct an Industry Benchmarking exercise to compare key payment metrics against industry peers (i.e., eCommerce payment approval rate, fraud losses, false decline rate, chargeback rate).

Expected Outcomes

- Payment KPIs compared to peer organizations along with a set of changes to enhance payment approval based on industry leading practices

3   Implement Right-Sized Solutions

- Leverage additional considerations like organizational factors and solution factors to identify the right-sized payment solution to simultaneously optimize revenue and mitigate fraud risk.

- Identify the appropriate application of Decision-as-a-Service (DaaS) for managing payment channels and mitigating fraud risk.

- Develop a prioritized implementation roadmap across people, process, and technology to maximize outcome and meet and/or exceed industry baseline.

Expected Outcomes

- Tailored approach to maximize approval rate while mitigating fraud and leakage

- Secure, efficient, and profitable payment ecosystem

- Prioritized and sequenced action plan to implement the identified tailored solution

Deloitte.

Deloitte helps clients design, build, and operate dynamic, business-aligned fraud programs for various line of businesses. You can be assured of being well equipped to meet the requirements, while continuing to focus on what you do best: managing your organization.

Deloitte's Financial Crime Practice is comprised of seasoned, senior professionals with hands-on, in-depth experience, leading various transformational Fraud initiatives at retail organizations, financial service institutions as well as the public sector.

Kevin Luh
Fraud Management Leader |
Financial Crime

416-824-1663
kluh@deloitte.ca

Jon Haywood
National Practice Leader |
Financial Crime

416-371-2311
johaywood@deloitte.ca

riskified

Riskified (NYSE:RSKD) empowers businesses to grow ecommerce revenues and profit by mitigating risk. An unrivaled global network of merchant brands partner with Riskified for guaranteed protection against chargebacks, to fight fraud and policy abuse at scale, and to improve customer retention.

Developed and managed by the largest team of ecommerce risk analysts, data scientists, and researchers, Riskified's AI-powered fraud and risk intelligence platform analyzes the individual behind each interaction to provide real-time decisions and robust identity-based insights

Kevin Sprake
Global Channel Partnerships Lead

732-241-3189
kevin.sprake@riskified.com

Ana Perez Mahiques
Director of Partnerships

917-991-3494
ana.perezmahiques@riskified.com