Deloitte.

Enhancing Issuer fraud strategy to improve Card Not Present Authorization Rates

Balancing Fraud Prevention and Consumer Experience

MAKING AN IMPACT THAT MATTERS since 1845

Contents

Key indicators of Card-not-Present (CNP) transaction conversion rates

Consumer experience is competitive advantage for CNP transactions

The increasing focus by merchants to improve online shopping experience with single click checkouts and refunds, personalized rewards, multiple payment options, digital wallet acceptance, logistics efficiencies, etc. have been instrumental in the exponential rise of e-commerce and the growth of Card-not-Present (CNP). While online transactions have been the default mode of purchase for younger generation, the digital divide between age groups is steadily contracting with Baby Boomers only marginally behind Millennials and Gen Z. By 2030, CNP transactions are expected to reach $17.8 trillion globally with ~19% projected CAGR[1]

Payment Approval

$17.8 trillion by 2030

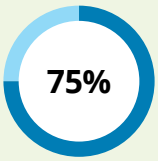
CNP transactions are expected to grow at a rate of ~19% CAGR to $17.8 trillion globally by 2030 up from $6.23 trillion in 2024[1]

Payment Fraud Losses

>$28 billion

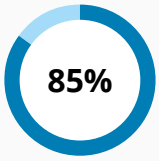
worth of global CNP fraud losses are expected by 2026[2]

False Negatives



Manual review of declined transactions by issuers reveal **that 3 quarters of those transactions were legitimate and would have been approved if Fraud controls were** accurate[6]. Nearly 10% of all e-commerce revenue is rejected by fraud detection systems.

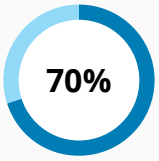
Payment Approval



of the CNP transactions get approved

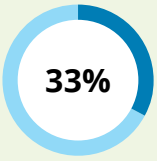
This rate lags other forms of payments such as card-present payments which see more than 96% of its transactions authorized[3]

Fraud Prevention



CNP crime accounts for almost 7 in 10 fraud losses to merchants and acquirers[4]

Customer Retention



of the customers end up seeking competition when they experience decline[5]

As the physical card is not presented for authentication and authorization at the time of purchase for a CNP transaction, risk of fraud is high. Issuer strategies to combat this risk very often leads to high false negatives and lower conversion rates as compared to card present transactions. Focusing on reducing the false negatives (~75%) can help to improve checkout experience and retaining the customers[6]

The impact of issuer fraud strategy on consumer experience

Issuer fraud strategy will be key in maximizing the returns from the growth in Card-not-Present transactions

> Consumer expectations have evolved with the growth of online shopping, and projections indicate substantial future growth in global and US B2C e-commerce markets by 2030.

Global B2C e-Commerce Overview[1]

Market size - **19.1%** anticipated growth rate

$6.23 trillion
2024

$17.8 trillion ▲
2030

US B2C e-Commerce Overview[1]

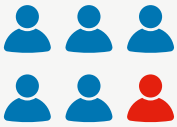
Market size - **15.5%** anticipated growth rate

$1.4 trillion
2024

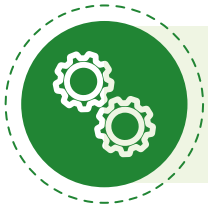
$2.8 trillion ▲
2030

With the surge in digital transactions, Issuers need to streamline fraud strategies to mitigate monetary losses while trying to tackle implications on customer experience and keeping operational costs low

E-commerce payment rejection rates are 15%, about 10% higher than in-person transactions, causing **issuers and merchants to lose out on billions of dollars** in transactions each year.[3]



1 out of 6 consumers face a False Decline[9]



To combat the rise in fraud, issuing banks often employ **conservative logic** when approving CNP transactions leading to declining of valid transactions from legitimate customers.

Lower authorization rates, increased online fraud, and poor checkout experiences financially impacts card issuers and merchants with **negative implications on customer experience.**

Current Fraud strategies have added friction during checkout experience

Conservative authorization strategy and traditional step-up challenges are degrading the consumer experience, causing frustration with cardholders and loss of coveted "top of wallet" status for issuers.

3D secure 2.0

- **46% of 3DS 2 authentications** take longer than 5 seconds[11]
- **22% of the transactions are lost**/abandoned[11]

70%

or more card holders approach their card issuers first when they are unsure of a transaction on their statement[10]

Traditional Multi factor Authentication

- **62% of the customers today want a secure option** that isn't traditional MFA[12]
- **Only 60% customers enable MFA** for Online Banking[12]

33%

customers decline MFA because it is annoying[12]

Conservative Authorization Strategy

- **61% of users** who didn't manage to conduct a transaction due to the false positive blocking, **cut down on card usage or stopped using** them all together[5]
- **40%** of the customers who experienced a decline on their first visit **will not revisit a Merchant's site**[10]

33%

of the customers end up seeking competition when they experience decline[10]

Poor customer experience translates to lower cardholder retention
Consumers face pain points like **transaction declines and cumbersome authentication processes,** resulting in reduced customer retention and loyalty to a specific credit card issuer. **Difficult checkout experiences cause higher attrition rates,** as customers today have many choices between different card issuers.

Strategies to improve authorization rates

Issuer fraud strategy should be optimized to improve authorization rates and checkout experience critical to retain customers

> According to a PYMNTS Intelligence report, 47% of retailers reported that false declines negatively impact customer satisfaction. Additionally, 58% of small and medium-sized businesses (SMBs) indicated that these declines have a substantial impact on their operations[13].

Issuers have an opportunity to optimize their strategies

Streamline integrations with ecosystem partners to enhance authorization data and streamline authentication flows

+

Utilize AI and machine learning to improve processing efficiency for large amounts of data

=

Key Outputs

- **Improve authorization rates**
- **Reduce fraud losses**
- **Enhance fraud prevention**
- **Reduce chargeback costs**
- **Enhance customer satisfaction**
- **Improve operational efficiency**

In US, potential value that can be retained from addressing false decline is **$16.5 Bn**[1, 3, 6]

Globally, the potential value that can be retained from addressing false decline is **$73.3 Bn**[1, 3, 6]

Streamline integrations with ecosystem partners to enhance authorization data and streamline authentication flows

> Issuers can significantly reduce fraud losses, improve authorization rates, and enhance customer satisfaction by integrating advanced fraud detection and prevention tools, and collaborating with merchants.

Issuer collaboration with ecosystem partners is demonstrating to be an effective strategy in reducing friction in the checkout experience while combating fraud and chargebacks. For example, Riskified's Adaptive Checkout, screens fraudulent behavior against pooled data from participating merchants before it reaches the issuer's authorization systems. It additionally sends enriched order data to participating issuers, helping them to weed out false positives and improving conversion rates.

- **Segmentation engine for authorization:** Issuers should consider the use of cardholder behavior data and spend patterns by working alongside industry players. This can help to provide better customer experience for issuer and merchants, and improve authorization rate for online transactions. Issuers should consider embedding a **segmentation engine into their authorization strategy to** predict their cardholder behavior **using consolidated data**.
- **Use of Network Tokens and Push Provisioning:** Issuers are promoting the use of network tokens with their customers and offering the ability to **'push' a token directly from the issuer's mobile app to a merchant,** reducing the friction of keying in card details during online checkout. These tokens also remain updated when new card numbers or expiration dates are updated. These tokens can improve authorization rates by up to 4.3% and reduce friction at the point of sale.[16]

Industry Insights

60% of merchants' plan to increase their spending on fraud management tools and technologies over the next two years.[17]

Capital One Direct Data Share (DDS) through partnerships with Stripe and Adyen designed a tool to enhance credit card payment authorization decisions in real-time, aiming to reduce fraud losses and false declines for merchants. The solution has already demonstrated its efficacy, **facilitating over USD 1 billion in merchant transactions that would have otherwise been declined.**[14]

Secure Payment Confirmation (SPC) via WebAuthn is revolutionizing payment **authorization by incorporating cryptographic authentication and biometrics.** In 2020, Stripe conducted an experiment with SPC in their production environment as part of Chrome's origin trials. The results were impressive, with **an 8% better conversion rate and a checkout rate that was three times faster.**[15]

Utilize AI and machine learning to improve processing efficiency for large amounts of data to reduce false declines

> The adoption of AI-driven tools for transaction monitoring presents a transformative opportunity for issuers that can significantly enhance fraud prevention, improve authorization rates, reduce charge-back costs, and improve overall operational efficiency.

AI-driven analytics play a crucial role in transaction monitoring by remaining vigilant in real-time transactions. AI can detect variations that are likely to present uncharacteristic trends, **such as..**

- **Unexpected Purchase Behavior:** Identifying anomalies in purchasing patterns that deviate from typical customer behavior
- **Disparities in Billing Information:** Detecting inconsistencies in billing details that may indicate fraudulent activity
- **Geographic Activity Surges:** Monitoring sudden increases in transaction volumes from specific geographic regions or IPs
- **Device behavior:** Monitoring for anomalies in device usage patterns (for example, an iOS user suddenly makes a purchase using an Android device with older OS version)

.... using various Monitoring models like

- **Network Analysis:** AI models analyze transaction networks and relationships between different entities to identify patterns of fraudulent behavior
- **Machine Learning Models:** Machine learning models are trained on transactional and customer interaction data to detect suspicious patterns and anomalies
- **Behavioral Analysis:** AI-powered systems utilize machine learning techniques to build profiles of normal customer behavior and detect anomalous activity
- **Biometric Authentication:** AI-powered biometric authentication methods verify the identity of users during transactions, reducing the risk of identity theft and account takeover fraud

Industry Insights

97% of organizations report missing valuable opportunities due to gaps in transaction data

Stripe's Radar **uses machine learning to analyze transaction data points across millions of companies,** flagging potential fraud in real time. The most important aspect is its ability to **learn from a global dataset of transaction patterns,** to better identify legitimate transactions. This significantly **reduces false declines by improving fraud scoring accuracy** and enabling dynamic, data-driven decision-making.

NuData implemented a behavioral biometrics solution to address fraud concerns for a client bank. The biometric algorithm created **user profiles in 30 days.** After deploying the solution in the bank's login process, the bank saw **91% of its users recognized and a 0.01% false-positive rate.** This technology has broad applications including identifying user patterns during checkout such as keystroke & touchscreen dynamics.[18]

Conclusion and Considerations

Drivers for efficient fraud control

> Issuers should consider technological, privacy, regulatory and governance implications before adopting consolidated data and insights approach to reduce fraud.

Comprehensive Transaction Metrics

Access to a panoramic view of actionable transaction metrics and consumer behavior data available to issuers offers a unique opportunity to mitigate fraud

Continually Optimizing Fraud Strategy

Identifying new trends as they emerge and adjusting anti-fraud operations, accordingly, will help in reducing friction for all stakeholders and providing improved efficiency, minimizing the impact of fraud and improving customer experience

Key Considerations

Technology

Technology and Infrastructure
Leverage open banking and service-oriented-architecture to build solutions on future-proofed footing and invest in device first strategy.

Market solutions
Evaluate in-market solutions and identify opportunities and strategic partners to go-to-market with new solutions.

Interoperability
Use accepted industry-standards to ensure systems are interoperable within the ecosystem.

Privacy

Data Privacy across organization
Implement homomorphic encryption, differential privacy, and secure multiparty computation to ensure privacy across parties.

Regulations
Assess the regulatory landscape of new technology like AI before making large investments.

Consumer perception
Ensure consumer experiences are thoughtful, will be seen in a positive light, and not seen as invasive or creepy.

Controls & Governance

Decision management policies
Define clear business and technical controls for workflow decisions made with AI and ML.

Identity & access controls
Ensure access to consolidated data sources by implementing robust security policies for Role based Access, authentication, and verification.

Governance
Implement AI governance processes that evaluate LLMs, models, and rules to ensure solutions continue driving their desired outcomes.

Endnotes

1. "B2C E-commerce Market Size, Share & Trends Report, 2030", Grand view Research, Forecast period (2024-2030)
2. "3 Chargeback Trends And How to Be Ready for Them", Ethoca, October 11, 2023
3. Juan G. Martín Escolar, "Maximize Your Approval Rates: A Guide for Merchants", PayU GPO, June 13, 2024
4. "Seven card-not-present fraud trends and ways to manage risk", Mastercard, 2025
5. Ivan Vorobyev and Anna Krivitskaya, "Reducing false positives in bank anti-fraud systems based on rule induction in distributed tree-based models", September 2022
6. "Seeing Revenue Loss Resulting From False Declines? The Solution May be Right Around the Corner", Chargebacks911, February 6, 2023
7. "Generational Divide in Online Shopping? Not So Fast, Says New Report", PYMNTS, January 22, 2025
8. "eCommerce for All: How Consumers Across Generations Make Purchases Online", PYMNTS, January 2025
9. "The E-Commerce Fraud Enigma: The Quest to Maximize Revenue While Minimizing Fraud", Experian, August 1, 2022
10. "Four trends shaping the future of fraud prevention, chargeback reduction and the omnichannel approach to digital payments", 2023 Payments market Outlook by Ethoca, 2023
11. "3DS, PSD2 and strong customer authentication", Ravelin Insights, accessed on June 13, 2025
12. "State of MFA Report", Prove Identity, 2023
13. "47% of Retailers Say False Declines Impact Consumer Satisfaction", PYMNTS, January 14, 2025
14. Amelia Matthewson, "Fighting Fraud: Capital One, Adyen and Stripe Share Data", June 6, 2024
15. Eiji Kitamura, "Secure Payment Confirmation", Chrome for Developers, May 27, 2022
16. "Drive value and revenue with secure and seamless payment experiences for your customers", Visa, accessed on June 13, 2025
17. Keri Kramers-Dove, "How Visa can protect you against unprecedented fraud", Visa Acceptance Solutions, June 24, 2024
18. "How a bank delivered a better user experience to 91% of its users with behavioral biometrics", NuData Security by Mastercard, February 2022

For more information please contact:

Sohail Kagzi
Consulting Managing Director
Banking & Payments
Deloitte Consulting LLP
skagzi@deloitte.com

Satish Lalchand
Advisory Principal
Banking & Payments
Deloitte Consulting LLP
slalchand@deloitte.com

Shereena Sherafudeen
Manager
Banking & Payments
Deloitte Consulting LLP
ssherafudeen@deloitte.com

Shalvi Saruparia
Manager
Banking & Payments
Deloitte Consulting LLP
ssaruparia@deloitte.com

Mohit Porwal
Senior Consultant
Deloitte Consulting LLP
pomohit@deloitte.com

Jeremy Firns
Senior Consultant
Deloitte Consulting LLP
jfirns@deloitte.com

Sriram Sukumar
Consultant
Deloitte Consulting LLP
srsukumar@deloitte.com

Rajeev Rishi
Analyst
Deloitte Consulting LLP
rirajeev@deloitte.com

Justin Tsang
Analyst
Deloitte Consulting LLP
jutsang@deloitte.com

Apoorva Aggarwal
Senior Consultant
Deloitte Consulting LLP
apoaggarwal@deloitte.com

Deloitte.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

CoRe Creative Services. RITM2112842