24
Jun

Safeguarding E-commerce: Strategies to Combat Card-Not-Present Fraud

Online payment fraud is projected to reach $200 billion by 2025, making robust measures like multi-factor authentication and AI-driven monitoring essential.

Christopher W. Knight
CFE, CAMS, CFCI, CHTI, CCTA
Founder & President at
Knight Vision Fraud Investigations

$200,000,000,000. Or for those like me who prefer it written out, $200 billion. That's the staggering amount estimated to be lost globally to online payment fraud by 2025.[1] To put that into perspective, it's nearly enough pennies to reach the moon if you were to stack them on top of each other. It's also around 3.6% of retail e-commerce sales globally, a figure that can skyrocket to 20% in markets like Latin America.[2,3] Truly "out of this world."

This means that for every $100 sold, merchant lose $3.60 to fraudsters. Combined with the 2%-5% average Merchant Discount Rate (MDR) businesses pay to collect payments online, operational costs related to payment acceptance can climb to

nearly 9%. This is unsustainable, especially for small businesses, and a massive challenge for payment processors.

The Threat Landscape for Payment Service Providers

So, what risks do payment service providers (PSPs) face in this context? Two significant ones stand out:

1. **Excessive chargebacks due to a merchant's financial and product mismanagement**
2. **Onboarding of fraudulent or misleading merchants**

As an e-commerce card-not-present (CNP) service provider, can you reduce your risk? Despite the increasing sophistication of CNP fraud, the answer is a resounding yes!

The Rise of CNP Fraud

Why is CNP fraud escalating? Fraudsters are undeterred by failure and have a wealth of lucrative schemes at their disposal. Faster payment settlements, like Brazil's instant payment system (PIX), make it easier for fraudsters to make near-instantaneous transfers, attracting those with unscrupulous intentions.

The digital world has made CNP fraud scalable, with compromised card numbers available to purchase for as little as $8 and payment data for around $220 on the dark web (a topic for another day). As consumers flock to user-friendly digital options, fraudsters follow, using advanced technologies like AI to conduct fraud attempts with minimal effort. In the United States alone, "60% of U.S. credit card holders have been victimized by fraud, and 45% have experienced fraud multiple times" per Security.org's 2023 Credit Card Fraud Report.[4]

With that, let's dive into three main issues driving substantial losses and explore solutions to mitigate them: Account Takeover (ATO), chargebacks, and Synthetic Identity Fraud.

Account Takeover (ATO)

What is ATO?

Account Takeover occurs when a malicious actor gains access to a user's account credentials and takes over the account without consent. The most common method in a CNP environment is phishing, where fraudsters impersonate trusted entities to obtain sensitive information like usernames and passwords, but a new trend has emerged in which AI is being used to create "deepfakes"- live video altered to look and sound like someone else. Don't believe me? A multinational firm in Hong Kong was just tricked into paying $25M to fraudsters after they were able to impersonate, among others, the CFO on a live video chat![5] This is going to take some effort for banks and others to detect and, simply put, is scary.

What can e-commerce PSPs offer to their merchants to mitigate potential losses?

Multi-Factor Authentication (MFA): MFA enhances verification by using dynamic, behavior-based credentials, and transcends beyond static passwords significantly mitigating phishing risks.[6]

Biometrics and Device Fingerprinting: Utilize biometric features like fingerprint scans or facial recognition. Device fingerprinting, which identifies unique device attributes, can detect unusual logins or activity, signaling unauthorized access.

Transaction Monitoring: Implement AI-enabled transaction monitoring and static suspicious activity alerts. Use behavior trends to identify unusual transaction patterns, such as sudden increases in transaction volume or value.

Chargebacks – "Friendly Fraud"

What is friendly fraud?

Friendly fraud occurs when a cardholder claims a legitimate transaction is fraudulent, often due to buyer's remorse. According to a 2020 FIS Global report, friendly fraud accounts for up to 70% of all credit card fraud, costing the industry nearly $132 billion a year.[7,8] Ensuring merchants are delivering quality products, engaging in prompt two-way active communication with customers, and issuing refunds when appropriate are the most effective ways to reduce the chances of friendly fraud and keep good customers, but it surely won't eliminate it.

What should a PSP ensure their merchants are doing to reduce their risk?

Customer Segmentation: Classify your customer base into high, medium, and low-risk tiers. Implement different friction points for each segment to detect signs of fraud more effectively, giving special diligence to new accounts.

Data Capture: Collect comprehensive data points during the customer journey, such as personal identifying information (PII) and IP/geolocation information, to create fraud alerts and respond to chargebacks effectively.

Restrict Access: Don't hesitate to restrict or terminate access for customers who frequently file chargebacks, especially ones who engage in friendly fraud. This can prevent recurring issues and save costs in the long run.

Document and Fight Chargebacks: Maintain thorough documentation for each transaction and submit it as evidence during chargeback disputes. PII, IP information, and transactional activity patterns are crucial for winning disputes as they show an additional pattern of behavior.

Synthetic Identity Fraud

What is synthetic identity fraud?

Synthetic identity fraud involves creating a fictitious identity using a combination of real and fake information. This can include using a stolen social security number paired with a fake name, birthdate, and other details to open accounts, make fraudulent purchases, or build a credit profile. AI can even generate a fake human face to accompany these synthetic credentials, posing a significant threat. Over 80% of all new account fraud can be attributed to synthetic identity fraud with almost half of new account fraud occurring within the first day of opening.[9,10]

How can a PSP mitigate potential losses?

Identity Verification and Biometrics: Employ fast and reliable identity verification solutions that check multiple public and proprietary data sets against account-opening information. Biometric features like fingerprints and facial recognition deter fraudsters, as these are hard to replicate.

Optical Character Recognition (OCR): Streamline identity verification with OCR technology that captures information from data sources and verifies it against

government-issued documents.

Enhanced Due Diligence (EDD): Conduct thorough checks for new accounts. This can include phone verification, additional documentation requests, watchlist screening, and social media investigations. Fraudsters seek easy targets, so making the process rigorous can deter them.

To Implement or Not: That is the Question

First, let's establish a baseline for the industry. Speaking purely from an e-commerce standpoint, 3% of international orders were fraudulent in 2022. Where do each of your merchants stand on that spectrum? Are they above or below that mark? If they are below that 3%, does it mean they are on track or simply missing a lot of fraud? If they are above, is it due to faulty controls or insufficient investment in their fraud program? Dig deep and be honest with yourself—most likely, you and your merchants aren't investing enough in your fraud program and are losing more than you realize, regardless of where you fall on the spectrum.

Should you implement every strategy discussed or just one? The answer lies somewhere in the grey and depends on your specific situation. However, these fraud concerns are universal, irrespective of location, and some, honestly, are simply best practices for all industries worldwide.

Internal Alerting & Data Capture: This is a "must-have" regardless of company or merchant size. It requires minimal internal effort to build analytics and automated alerts tailored to your business operations. It's part of the basic foundation of any fraud program and doesn't rely on third parties, making it adaptable.

Identity Verification & EDD (Enhanced Due Diligence): EDD is another "must-have" for both PSPs and merchants of all sizes as it's a best practice and can keep regulators at bay. Identity verification is going to be outsourced and can be trickier thus is a "nice to have." Third-party systems like LexisNexis, especially in the US, are reliable but costly, usually as a pay-per-use service. Using it sparingly for high-risk customers can help you avoid sticky situations while also keeping costs low, however.

MFA & Biometrics: For newer or growth PSPs and merchants, MFA might add a bit too much friction when customer acquisition is going to be vital for sustainability. For more established entities, MFA incorporating biometrics and other options is a "must-have" due to its high efficacy in preventing fraud and its

relatively low cost—ranging from a few hundred to a few thousand dollars. This can be built in-house or purchased as a service, with the latter being more comprehensive. One concern is that advances in AI and "deepfakes" might make facial recognition the next likely target for fraudsters.

Device Fingerprinting: This 3rd party offering is on the verge of being a "must-have" and should be on everyone's roadmap for this year. It offers many benefits beyond fraud prevention, like marketing insights and user engagement, which can justify its cost. Services like Kount, which charge a few cents per transaction, provide valuable data and additional fraud rules.

Conclusion

As online payment fraud continues to evolve, the fight against it must also advance. By understanding the methods fraudsters use and implementing robust preventive measures, e-commerce CNP service providers can significantly reduce their risk. Multi-factor authentication, biometric verification, data-driven transaction monitoring, and enhanced due diligence are crucial tools in this battle.
Although the numbers are daunting, proactive and strategic defenses can help mitigate the impact of CNP fraud. The stakes are high, but with the right approach, businesses can protect themselves and their customers, ensuring a safer online marketplace for all.

Keep up to date with our e-commerce, payments and crypto insights:

Sources

1. LexisNexis, 2022. ↩
2. eMarketer, 2022 ↩
3. Jumio, 2023 ↩
4. Vigderman, 2024 ↩
5. Chen & Magramo, 2024 ↩
6. Vectra.ai, n.d. ↩
7. FIS/WorldPay, 2021 ↩
8. Mastercard, n.d. ↩

9. Purcell, 2023 ↩
10. Brighterion, 2022 ↩