E-BOOK

Advancing fraud protection with global network intelligence

Contents

Transaction-level and merchant fraud

$28.58b

Loss to card fraud, 2020, excluding other expenses (worldwide)

The Nilson Report, December 2021.

$408.5b

Estimated loss to card fraud, 2020-30 (worldwide)

The Nilson Report, December 2021.

Increased consumer demand for online sales and service and contact-free payments have changed the way merchants do business and complete transactions. Fraudsters are also taking advantage of this digital revolution to increase their gains.

There are many ways a fraudster can gain access to payment card credentials. These include card skimming, phishing, blunt-based bot attacks and account takeovers to name a few. Payments made with compromised cards that have been sold on the dark web or in the hands of fraudsters may be hard to detect.

Financial institutions (FIs), including acquirers, payment service providers and payment facilitators, must rely on intelligent fraud defense systems to determine genuine transactions.

FIs at risk: many shades of fraud and loss

Payment card issuers, who represent cardholders, reduced their fraud exposure with EMV chip cards by relying on merchants to verify user identity in the card-present world. In the card-not-present (CNP) environment, merchants and their acquiring banks carry that loss. Rising fraud, false declines and chargebacks create greater risks and rising costs for acquirers.

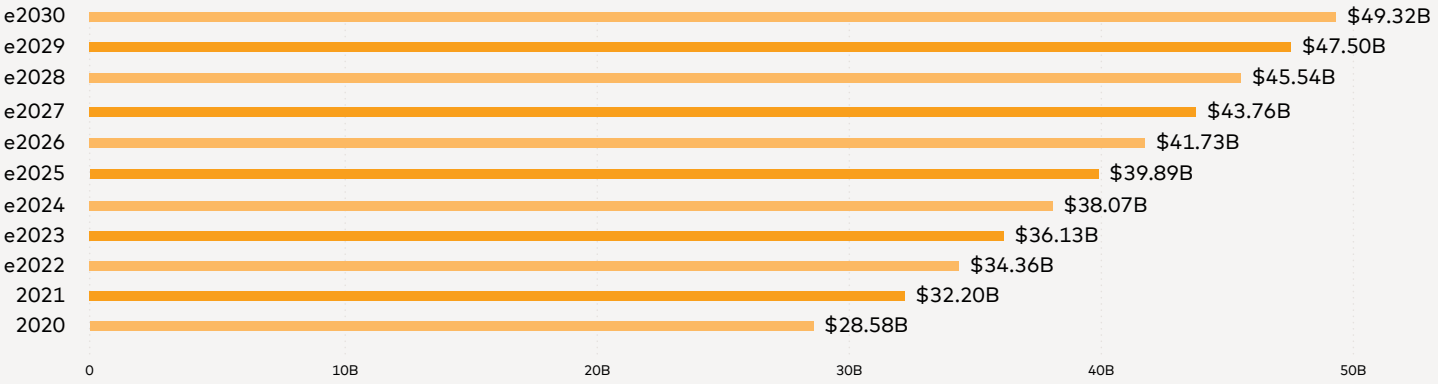
In 2020, $28.58 billion was lost worldwide to all levels of payment card fraud.[1] The onset of COVID-19 increased online commerce to 19 percent of total sales[2] (up from 15 percent in 2019). FIs faced a substantial risk of loss from CNP fraud.

As activity returned to pandemic-affected industries in 2021, attackers were close on their heels. And despite recent improvements in fraud management due to new technologies, criminals have continually become more sophisticated.

MRC[3] surveyed over 1,060 merchants from four key regions in December 2021. They found the percentage of eCommerce revenue lost to payment fraud globally was at 3.1% with KPIs for 2022 at 3.6%.

Projected global payment card fraud losses

(USD $billions)



Source: *The Nilson Report*, 2021.

Transaction-level fraud

Transaction fraud is the use of stolen or counterfeit credentials to make illegal transactions. Common examples of transaction-level fraud are:

1. **Clean fraud:** This method is difficult to detect because fraudsters use authentic – but stolen – credentials. In clean fraud, bad actors generally have a complete set of credentials, making it much easier to appear legitimate.

2. **BIN attacks:** BIN, or bank identification number, attacks involve using the first six numbers on a payment card which identify the issuing institution. Fraudsters use an algorithm to generate the potential remaining numbers, developing a list to use in card testing.

3. **Card testing:** Using stolen or generated credentials, fraudsters rapidly process small transactions to validate payment cards. A type of brute force attack, card testing identifies accounts that are active or have available funds. Card testing may take place with generated card information (e.g., BIN attacks), stolen cards or credentials purchased on the dark web.

4. **Card-not-present:** With purchases made online or over the phone, merchants are unable to verify a purchaser's identity. Estimated to be 81 percent of all transaction-level fraud,[4] CNP is difficult to detect unless payment systems flag transactions as suspicious.

Merchant fraud

Acquirers, PSPs and payment facilitators need to be on the lookout for fraud by merchants as well. Better insights into merchants' operational and fraud-related statistics are key. These insights help to identify potential vulnerabilities, revealing changes that may indicate fraud or collusion. Here are the five most common types of merchant fraud:

- **Transaction batch and credit abuse:** The merchant submits all transactions at once to bury a fraudulent transaction.

- **Bust-out fraud:** A fraudster applies for a merchant account without any intention of actually operating a legitimate business. These merchant accounts are then used to process fraudulent transactions or to acquire lines of credit before abandoning the account altogether.[5]

- **Identity swap fraud:** Individuals on the anti-money laundering/anti-terrorist funding (AML/ATF) watch list cannot open merchant accounts. These extremists often use fake or stolen identities to set up online retail sites to secure merchant accounts. These accounts may be used for money laundering.[5]

- **Transaction laundering (factoring or collusion):** The merchant processes transactions that the acquirer is not aware of, often unapproved or illegal transactions. Merchants may also be processing purchases for a third party for a fee.[5]

- **Business remodeling:** Once the merchant account is set up as a low-risk category business, the fraudster redesigns the business to sell goods of their choice. As low-risk businesses require less scrutiny, this is a very simple crime to commit.[5]

68%

Card fraud losses were CNP

The Nilson Report, December 2021.

60%

Merchants reducing/ eliminating manual review

Merchant Council, 2021

The challenge with current prevention practices

Transaction-level fraud

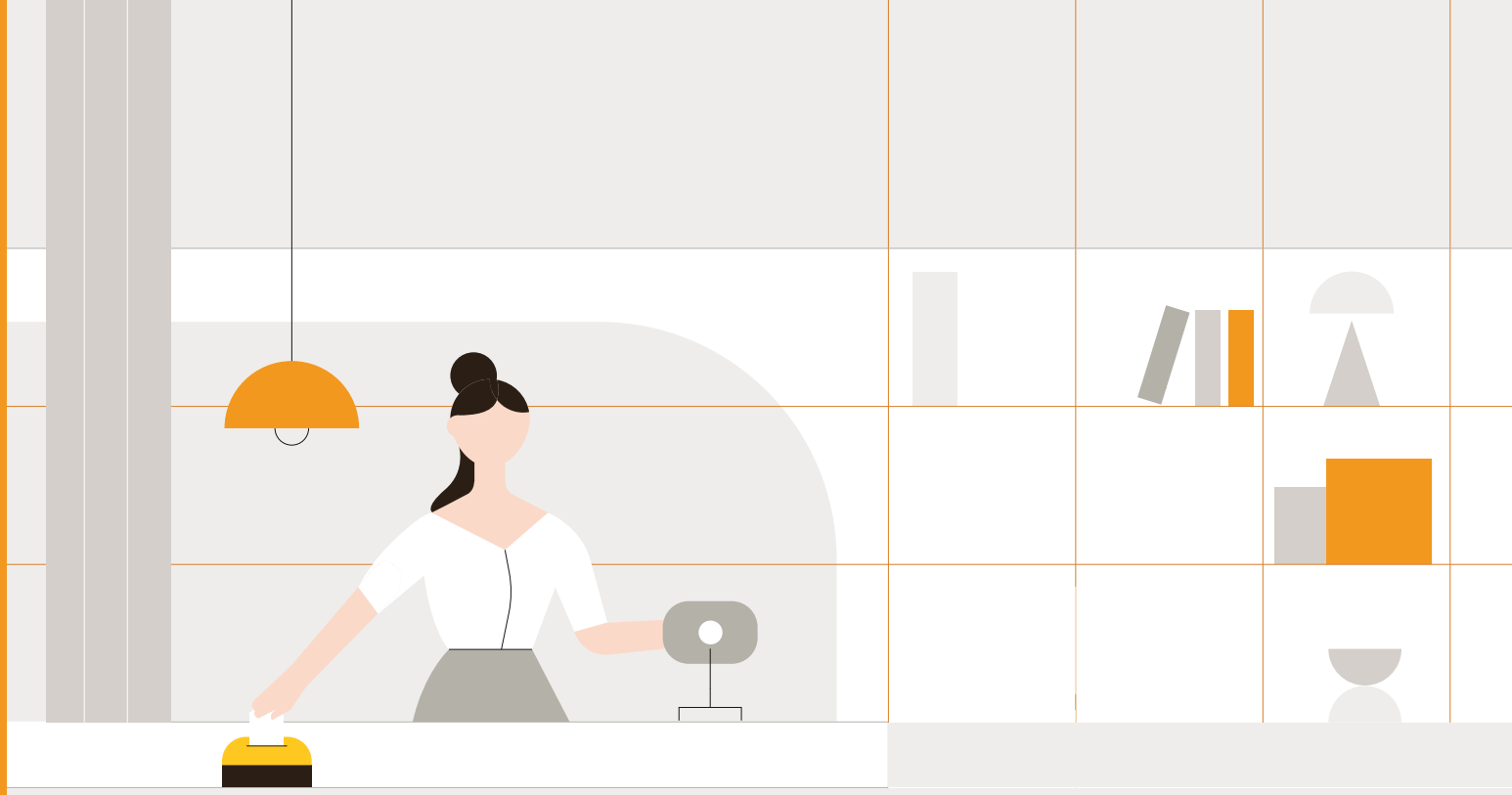
FIs endeavor to protect themselves and their merchants with AI solutions but are finding there is still room to increase transaction-level fraud detection and approvals while also reducing false declines.

Despite both consumers and fraudsters becoming more technologically sophisticated, one in four acquirers are relying on old solutions. According to the PYMNTS.com report, *AI in Focus: Waging Digital Warfare Against Payments Fraud*, 75 percent of acquirers say AI is an important or their most important tool to detect fraud, and 27 percent still use rules-based solutions as their primary fraud prevention system.[6] Acquirers are moving towards AI and are discovering the effectiveness of using AI in conjunction with rules and other legacy technologies.

The challenge with many solutions is they are trained for known fraudulent actions, and bad actors continuously evolve their behaviors to beat the system. As a result, some prevention solutions still return false positives at checkouts and miss many fraudulent transactions.

As fraudulent transactions still get through some existing payment defenses, merchants continue to rely on manual order review. However, Merchant Risk Council reports that 60 percent of merchants[7] plan to reduce or eliminate manual review, putting more pressure on FIs fraud solutions to be accurate and return fewer false positives.

A massive challenge is the amount of manpower needed to investigate the high volume of alerts, increasing merchants' overhead. It's not feasible to investigate them all. As a result, investigators overlook or miss many alerts that are triggered because they are unable to pinpoint the exact alerts.



Merchant risk management

Merchant risk management has its own set of challenges. FIs often rely on manual review, pulling reports to evaluate merchants' transactions and activities. While there are available solutions, many operate independently from the overall fraud prevention ecosystem.

Economic pressures, such as the results of lost business during crises like COVID-19 and cyclical recessions, put additional pressure on FIs to monitor merchants' behavior. Some FIs rely on their transaction fraud solutions to catch fraudulent merchants, while others resort to manual review for this purpose as well.

The time it takes to implement a separate merchant monitoring solution may be a barrier for busy FIs, although one could argue that time spent manually monitoring merchants' activities could be put to better use.

The value of customer retention

With the loss of customers and merchants comes a need to recruit new ones. Most sources cite a cost of at least five times to recruit a new customer over the cost to retain one, according to Invesp.[8] Their research also shows that while 44 percent of companies focus on customer acquisition, only 18 percent put emphasis on retaining those accounts.

However, the question remains: how do FIs proactively mitigate current and future losses while ensuring a seamless experience for their customers and merchants?

Proactive solutions for fraud prevention

"The pace of change has never been this fast, yet it will never be this slow again"

Justin Trudeau
Prime Minister of Canada

Constant change is a challenge in the payments business. E-commerce use is increasing, as is transaction-level fraud by criminals who recognize the opportunity. As discussed in Part One, the demand for online sales and services shows no sign of slowing down.

Forbes magazine quoted Canadian Prime Minister Justin Trudeau at the World Economic Forum: "The pace of change has never been this fast, yet it will never be this slow again."[9] The writer then noted, "That message rings true in payments, where each year the level of innovation and progress continues to accelerate, creating new market dynamics, opportunities and challenges for all participants." One year later the world faced a digital transformation accelerated by a global pandemic.

Recent events show that the fast-moving world in which we live and do business requires infrastructure and processes that keep up with rapid change. The dynamic environment of fraud and merchant monitoring requires proactive solutions that learn and evolve at the same speed.

Key features of Brighterion AI from Mastercard

- Full stack, state-of-the-art machine learning toolkit
- Customizable Rules Management, Case Management and Business Insights modules to enable flexible managing and reporting.
- Low latency of 100-120ms and less than 10ms when deployed on-premise.
- Unrivaled scalability and deployment
- Industry-leading data responsibility practice, with embedded human-centered data innovation and product design principles

Powerful cloud-based solutions enabled by Mastercard's global network intelligence

Advanced AI solutions must provide real-time decisioning to protect FIs and their merchants against loss. Exclusively trained on Mastercard's global network intelligence, Brighterion AI's solutions prevent fraud with more accuracy than ever before.

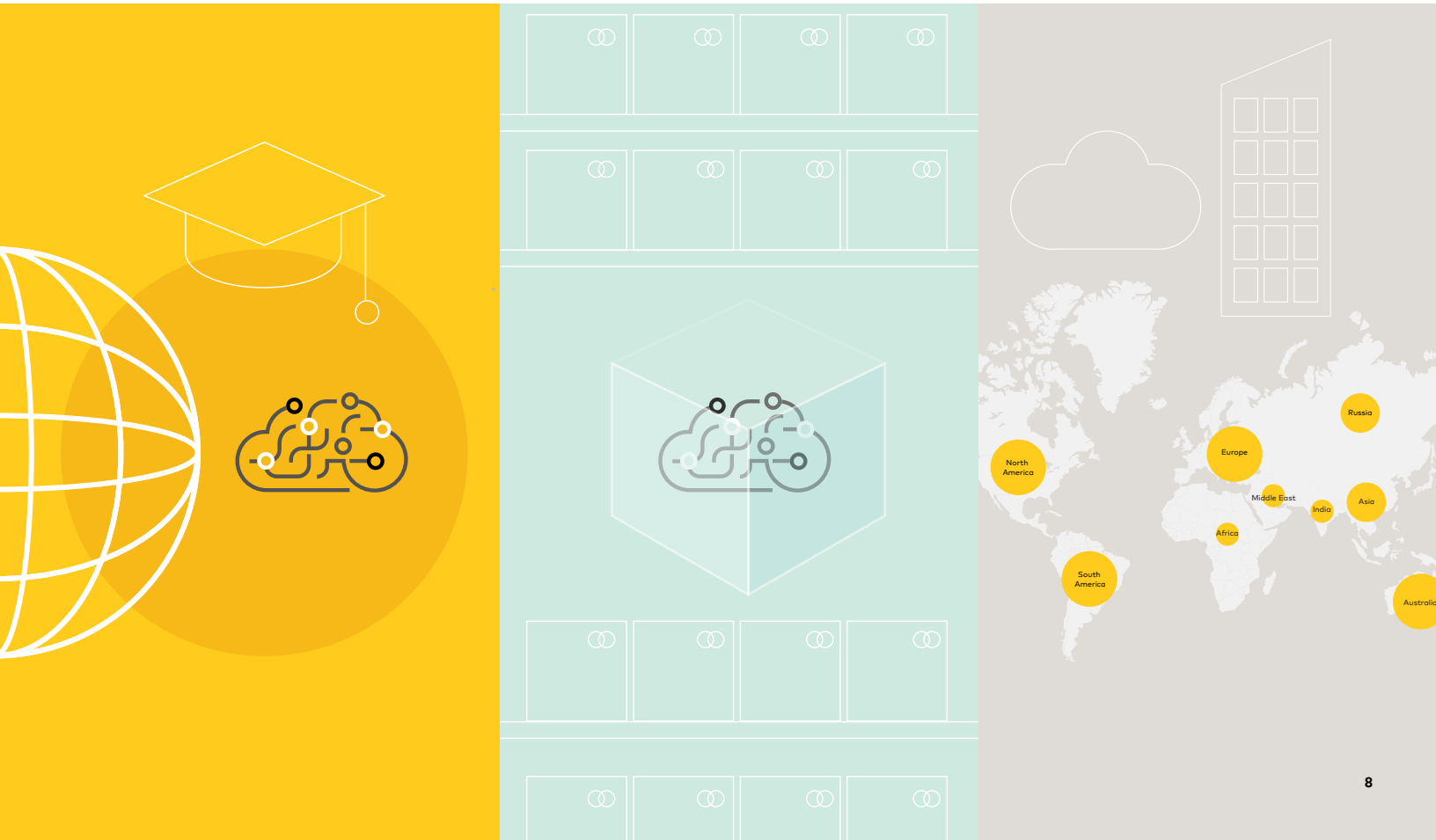
Mastercard data brings knowledge from the broader market to deliver fewer false positives and higher fraud detection rates.

With a network of 210 countries and territories, the breadth of transaction data is vast. Acquirers, PSPs and payment facilitators benefit from models trained to learn patterns and anomalies from anywhere in the world Mastercard does business.

Market-ready models: detect transaction-level and merchant fraud out of the box

FIs can now quickly respond to the threat of fraud with market-ready solutions. These AI and machine learning models are production-ready out of the box. They create a lighter lift and faster time to value than other solutions on the market.

While custom Brighterion AI solutions can be built to solve FI's specific business challenges, market-ready models can also be customized after launch to meet each FI's needs.



One global acquirer achieved:

2-3x

Increased fraud detection

7.4%

Increased approval rates

Transaction Fraud Monitoring: the most efficient way to fight transaction-level fraud

Brighterion AI for Transaction Fraud Monitoring helps acquirers increase approval rates and mitigate fraudulent transactions for their merchants by assessing the risk of transaction-level fraud earlier in the payment flow.

Trained on Mastercard's network intelligence, models have learned the most advanced fraud, including transactions that have slipped through other levels of payment flow security.

One major acquirer experienced two to three times increased detection rates and 7.4 percent higher approvals.

Key benefits

- Increases rates of fraud detection and approvals
- Saves time and money with fast and easy deployment
- Meets global compliance regulations
- Provides transparency with innovative explainable models
- Reduces losses by identifying fraud at the pre-authorization stage

One global acquirer achieved:

$50m

Savings YOY year in the U.S.

33%

Reduction in cases generated YOY

12%

Adverse Action Rate (AAR) = efficient case investigation

Merchant Monitoring: reduce merchant risk through continuous monitoring

Brighterion AI for Merchant Monitoring solution helps acquirers balance the potential of new revenue streams with the risk of fraudulent merchants by assessing existing and newly onboarded merchants. The solution analyzes each merchant's transaction patterns, providing risk scores that indicate the likelihood of merchants causing losses to the FI.

FIs can choose to have Brighterion AI monitor and score Mastercard transaction patterns on their behalf. This requires zero integration. Fraud analysts receive monthly risk score reports via Tableau, an interactive and intuitive solution.

Alternatively, FIs can fully integrate with Brighterion AI in a few simple steps and begin monitoring transactions from any card network.

Key benefits

- Saves time and money with zero integration; acquirers provide a list of merchants they would like scored
- Optimizes and empowers fraud analysts' investigations with accurate risk scores
- Improves results with a solution optimized specifically for merchant monitoring
- Enables flexibility with the ability to integrate an acquirer's historical data

Conclusion

"Our greatest return on investment from Brighterion AI is how we deploy the system, which is to do holistic merchant risk monitoring, so we aren't looking at singular transactions generally. We are looking at the performance of the entire merchant."

Jonathan Homer
Global Head of Analytics and Modeling, Worldpay

Brighterion AI monitors both transaction-level and merchant fraud. Market-ready AI models have been trained on Mastercard's decades of expertise in the payments ecosystem to detect fraud before it's processed.

For case-specific, unique challenges, Mastercard provides the AI Express process to quickly build and deploy custom AI models. These models can be ready for deployment within six to eight weeks.

When customer behavior changes, systems must be responsive through real-time decisioning to alert acquirers, PSPs and payment facilitators that consumers or merchants may be behaving in anomalous ways. Although the AI models have been trained on extensive transaction data, they continue to learn with each transaction.

These details are paramount for success, and it's important to have a fraud risk engine that scales reliably as threats evolve. Both increased threats and a growing customer base are factors that will affect your long-term investment. Brighterion's AI solutions are uniquely equipped to adapt to these ever-increasing risks and opportunities.

---

1. HSN Consultants, Inc., *Issue 1209, Nilson Report*, Dec. 2021.
2. Ibid.
3. Merchant Risk Council, *Global Payments & Fraud Report 2022*, (accessed 7 Sep. 2022).
4. U.S.News, "What is Card-Not-Present Fraud?" (accessed 2 Dec. 2022).
5. Pandey, Prachi. "What are Merchant Frauds: Types of Merchant Frauds and Measures to Tackle it." *SabPaisa*, 21 Jul. 2022 (accessed 7 Sep. 2022).
6. PYMNTS.com, *AI In Focus: The Rise Against Payments Fraud*, Dec. 2021.
7. Merchant Risk Council, *Global Payments & Fraud Report*, 2022.
8. Saleh, Khalid, "Customer Acquisition Vs. Retention Costs," *Invesp*, 11 Nov. 2019 (accessed 7 Sep. 2022).
9. McKee, Jordan, "Looking Backward To Move Forward: Payments In 2019," *Forbes Magazine*, 21 Jan. 2019.

** All Mastercard transaction data has been aggregated and anonymized when used to build Mastercard's AI and ML models.*

To learn more contact one of our AI experts → Visit our website →