UNDERSTANDING

THE TOTAL COST OF FRAUD

2018

Fraugster

ingenico ePayments

TABLE OF CONTENTS

04 Key Learnings

Merchants know all too well that keeping up with international consumer expectations is key to attracting and maintaining global shoppers. Merchant risk teams are often put under stress to keep up with the increased complexity of today's e-commerce world and have to deal with ever changing security risks. In such an evolving environment, modern fraud solutions can support and cultivate a merchant's business growth path. However, risk managers need to understand the requirements of how to best leverage fraud solutions to support their business.

Ingenico ePayments and Fraugster team up in the following report to first examine the true cost of fraud from Card Not Present (CNP) transactions, and then to discuss merchant concerns on how to adapt to new anti-fraud technologies in an exclusive interview.

KEY LEARNINGS

To understand the total cost of fraud, merchants must also consider prevention costs, lost revenue, and marketing expenses such as customer acquisition costs and potential damage to reputation.

New technologies can detect emerging fraud trends faster and more broadly than ever before.

As Artificial Intelligence (AI) enters the payment industry, the role of risk managers will evolve from operational tasks and building tools, to also include more insights-driven, strategic fraud prevention.

Fraud not only cuts into profits but also creates a poor customer experience when managed inadequately.

As shopping behaviors and patterns change, so do the challenges of fraud for merchants.

THE TOTAL COST OF FRAUD

THE TOTAL COST OF FRAUD

E-commerce sales are set to pass 4 trillion dollars worldwide by 2020, which illustrates the continued business opportunities for e-commerce merchants. However, the ongoing shift to online commerce also opens up new business to criminals.
It comes as no surprise that CNP fraud grows at a similar pace as the growing e-commerce market. In 2016 alone, merchants faced 33% more attacks than 2015, as reported by LexisNexis. [1]
When it comes to fraud management, merchants should be aware of the three cost factors that add up to their total cost of fraud:

1. DIRECT FINANCIAL COSTS

2. PREVENTION COSTS

3. LOST REVENUES

The composition of these three costs and the strategy of how to manage fraud varies greatly depending on business model, vertical industry, geography, payment method and types of fraud attack.

Merchants lose on average

1.5%

of their annual revenue to fraud attacks.[1]

[1] LexisNexis, True cost of fraud, 2016

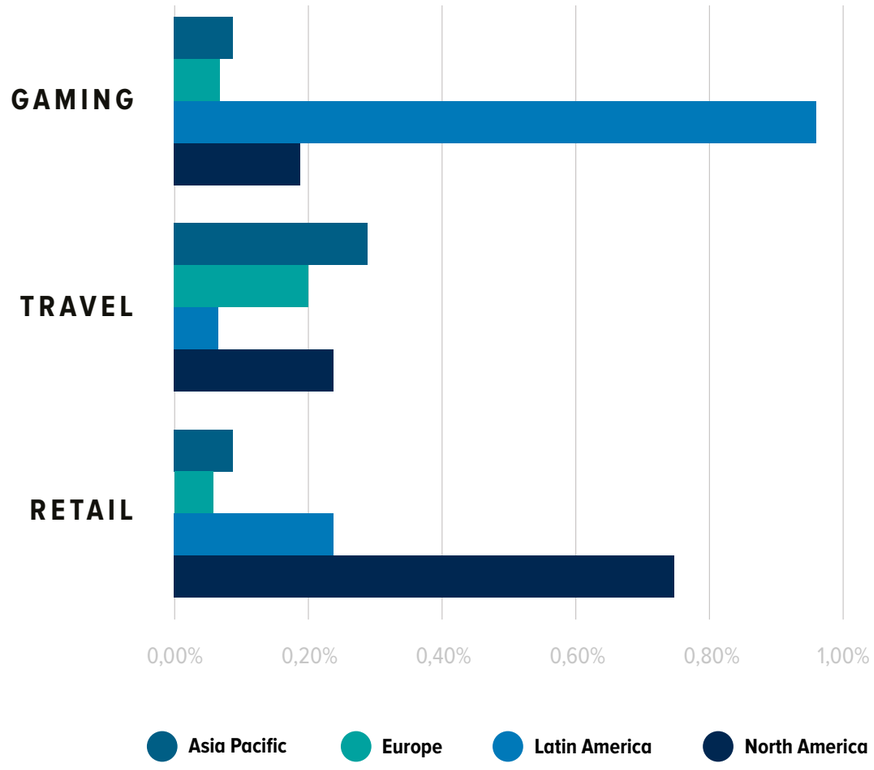
DIRECT FINANCIAL COSTS

Merchants lose on average 1.5% of their annual revenue to fraud attacks. This 1.5% represents product and service losses, chargeback fees, and potential scheme programs. [1] However, losses differ widely between industries, geographies, and time span. Furthermore, many merchants work with partners such as Ingenico and Fraugster to reduce their exposure to fraud. Data analysis from millions of online transactions processed by Ingenico shows that in 2016, an average retailer would have seen a swing in chargeback rates from as low as 0.08% to as high as 0.75%, depending on geography.

Across verticals, this same dynamism applies. For merchants processing payments from North America, chargeback rates were as low as 0.19% on average for video game companies, and up to 0.75% for online retailers.

CHARGEBACK RATES IN 2016

Ingenico ePayments merchants by vertical and region



BREAKDOWN OF FINANCIAL COSTS:

1. PRODUCT & SERVICE LOSSES

Covers sales revenue that is at risk of being stolen; this also includes shipping costs of physical goods that were already sent by the time a chargeback occurred.

2. CHARGEBACK FEES

If a cardholder disputes a transaction the resulting refund initiates a chargeback. The fee usually ranges between $20 - $50 per chargeback and can be broken down between card scheme, acquirer and processor.

3. CHARGEBACK PROGRAMS

Merchants that are not compliant with chargeback or fraud requirements of card schemes like Visa or Mastercard, face additional charges. For instance, if a merchant's chargeback rate is over 2%, Visa will start an excessive chargeback program which can result in tens of thousands of dollars in penalties. Each card scheme has its own indicators that can trigger the start of a chargeback program which could potentially lead to exclusion from that scheme.

PREVENTION COSTS

Anti-fraud technologies are constantly evolving and to ensure that all payments are protected, merchants must find the right balance between tools as well as external and internal expertise. In order to effectively verify single CNP transactions, e-commerce merchants can consider four common approaches:
Each approach can be mixed, matched and enriched with additional tools such as device ID fingerprinting, 3D-Secure, digital identity or geolocation.

MANUAL REVIEW

Human analysts review transactions manually.

STRENGTH: Highly accurate.

WEAKNESS: Not scalable to large volumes. On average each analyst needs 1-2 minutes per transaction, totaling around 200-250 orders per day with the right tooling.

RULE BASED

Human analysts define rules for single cases.

STRENGTH: Flexible approach for specific users or industries.

WEAKNESS: Significant expertise and manual effort needed to define and maintain rules.

MACHINE LEARNING

Fixed statistical models trained with minimal human involvement.

STRENGTH: Highly scalable.

WEAKNESS: Models need to be adapted manually and therefore require manpower and expertise.

ARTIFICIAL & BEHAVIORAL INTELLIGENCE

No predefined models that identify fraud patterns automatically.

STRENGTH: Highly scalable and flexible.

WEAKNESS: Requires large amount of data to be effective.

Choosing the right approach becomes even more complicated once merchants start a make or buy discussion. Merchants should consider three different costs associated to make this decision:

- *Cost of external prevention tools*
- *Cost of developing internal prevention tools*
- *Cost of managing and maintaining the tools*

Choosing the right approach becomes even more complicated once merchants start a make or buy discussion.

COST OF FALSE POSITIVES & LOST REVENUES

The true cost of fraud isn't limited to direct financial costs, but also includes the cost of missed sales opportunities. False positive transactions occur when a fraud prevention tool mistakenly considers an innocent transaction as suspicious and blocks it. False positives equal lost sales revenue for merchants, and thus can have a tremendous impact on a merchant's bottom line. So for merchants, it is not enough to have the right tools and expertise to minimize fraud, but also to ensure that genuine transactions don't get declined. Authentication tools can be used to minimize the risk, but they tend to add friction to the payment experience, leading to consumer drop off and lost revenues. Getting the balance right is critical.

BREAKDOWN OF FALSE POSITIVE COSTS:

1.

LOST REVENUE

According to research by Javelin, 15% of all cardholders have experienced at least one declined transaction. [2] Fraud prevention tools can heavily impact a merchant's decline rate and result in less revenue. Many merchants still overestimate fraud losses and underestimate their revenue losses through false positives.

2.

ACQUISITION COST

Considering the long journey a customer takes from comparing prices and products to purchasing, lost sales from a fraud solution can be especially damaging. Customer acquisition cost (CAC) is one of the most important KPIs for e-commerce retailers and is usually accompanied with a large marketing budget. If a customer is then not able to finalize a purchase due to a fraud prevention system, the invested money is lost and the CAC is increased.

3.

REPUTATION DAMAGES

Behind every false positive transaction is a disappointed customer who couldn't complete a transaction. Such situations damage a merchant's reputation and diminish a customer's trust. Six out of ten customers will shop less or will never return to a merchant who blocks their transaction.

6 out of 10

customers will shop less or will never return to a merchant who blocks their transaction.[2]

[2] Javelin, Overcoming False Positives: Saving the Sale and the Customer Relationship, 2015

TRENDS & CHALLENGES

CROSS-BORDER PAYMENTS

TRENDS & CHALLENGES:
CROSS-BORDER PAYMENTS

According to a new report by DHL, cross-border e-commerce growth is set to surpass domestic online retail with a predicted worth of $900 billion by the end of the decade. [3]

While cross-border shopping represents a significant growth opportunity, it also introduces new and unique challenges associated with new market dynamics. Just as they have to adapt to different currencies and payment options, merchants also have to approach fraud differently.

Finding a fraud solution that can adapt to these changes is not an easy task. Though many merchants acknowledge the changing face of retail, all too often they do not move fast enough to keep ahead. Fraud management can determine the success of a new market launch and challenge an organization on many levels. Taking the example of risk managers using classic rule based solutions for cross-border payments, they will face the following challenges:

By entering a new market, you open up new shopping behaviors and with them new fraud patterns.

If existing rules don't fit a new market a merchant will be hit hard by lost revenues as they will be blocking too many good customers.

Risk managers need to have extensive knowledge of shopping behaviors in a variety of markets.

As each market differs and changes with cross-border payments, risk managers need to find the right approach to minimize cost and maximize revenue.

Cross-border e-commerce growth is set to surpass domestic online retail with a predicted worth of

$900bn

by the end of the decade. [3]

[3] DHL, The 21st Century Spice Trade: A Guide to the Cross-Border E-Commerce Opportunity, 2016

FINDING
THE RIGHT
APPROACH

Exclusive interview with

Sasha Pons, Director of Product-Fraud Prevention Solutions at Ingenico ePayments

& Chen Zamir, CTO and Co-Founder of Fraugster

EXPERT INTERVIEW

Considering the complexity of the total cost of fraud, fraud management in itself can become a bigger problem than the initial fraud attack.

Fraugster, a German-Israeli payment security company, believes that e-commerce merchants should not have to worry about the cost of fraud. Fraugster's Fraud Free Product is based on a proprietary Artificial Intelligence technology that is so precise it allows Fraugster to take over merchants' fraud losses and reduces operational costs.

As the Director of Product - Fraud Prevention Solutions for Ingenico ePayments Sasha Pons works with merchants to find the best fraud solution for their business by focusing on three core areas:

- *Maximizing the number of approved transactions*
- *Minimizing the cost of chargebacks, and*
- *Reducing the operational cost of running a fraud department*

To that end, Sasha's team of dedicated fraud expert partners with industry-leading fraud detection solutions such as Fraugster to provide merchants with the optimal balance between fraud protection and sales conversion.

Today, the buzz of Artificial Intelligence (AI) has some merchants nervous about trusting a new technology and they are hesitant to move towards an AI focused future.

- Chen Zamir, CTO and Co-Founder of Fraugster, is actively shaping this future. As veterans in fraud management, Sasha and Chen take on merchants commonly asked questions about Artificial Intelligence. During which, they also examine Fraugster's approach compared to classical solutions and explain how the technology is changing the role of fraud manager.

Sasha Pons

Compared to classical solutions how is it possible to detect fraud trends that have never happened before?

Chen Zamir

You cannot detect new fraud trends by only looking at historical transactions and patterns. To be able to detect new trends, Fraugster has developed a set of features like outlier detection and network analysis, to recognize new user behaviors. Fraugster can detect even the smallest changes in shopping behavior which means we can track and assess the risk, and as this process is fully automated our engine becomes smarter with every transaction.

Sasha Pons

To detect fraud you require behavioural intelligence. Are computers sophisticated enough to do that?

Chen Zamir

Yes they are, as long as you focus on a very specific problem. In Fraugster's case, our machine specifically recognizes shoppers with stolen credit cards. Let me explain it with an example:
Say I am on holiday back in Tel Aviv and I want to buy a laptop from a UK website with my German credit card. Many fraud solutions would flag this transaction as suspicious and think this is a stolen card. Comparatively Fraugster's behavioural intelligence engine will look into the story behind the transaction. The engine will recognize that Chen is an Israeli name, it will also recognize that I am using an IP connection from a hotel and that my shipping address is a German one. From this perspective the transaction no longer looks suspicious and Fraugster will approve it.

> **"THE JOB OF A RISK MANAGER IS NOT TO BUILD THE TOOL, IT IS TO UNDERSTAND THE FINAL RESULT AND THEN DECIDE HOW TO USE IT.**

Sasha Pons

Most fraud managers are not trained data scientists. Is this a requirement to use and work with a technology like yours?

Chen Zamir

No, definitely not. The job of a risk manager is not to build the tool, it is to understand the final result and then decide how to use it. For technology companies like us we have to keep the actual user, risk managers, in mind and thereby we've built our algorithm as a white box. This allows us to translate machine insights into human actionable knowledge.

Sasha Pons

What exactly do you mean by white box? Why is it so important in the context of AI?

Chen Zamir

A white box is a completely translucent set up where risk managers not only get a score but they also see the reasoning and logic behind it. It is not enough that an algorithm outputs a cryptic score but it needs to convey, in human context, why it gave this feedback.
At Fraugster, we have developed an AI technology that is empathetic to the fraud manager who works with it. Without a white box our results would be questioned and not trusted.

Sasha Pons

Can you give us an example?

Chen Zamir

Let's take a transaction with a suspicious e-mail address. A solution that uses a black box will only indicate that the transaction looks suspicious. Obviously, that is not very helpful for a risk manager, as it doesn't explain what exactly is suspicious about the transaction.
A thorough understanding of why the machine came to a certain conclusion is important. In the case where a legitimate transaction is blocked, you will want to understand why it was blocked so that you, as a risk manager understand what needs to be fixed. In this case a white box like that of Fraugster's will be able to explain to a risk manager that not only is the email suspicious but also why the email was suspicious. For example, the email address did not match the name of the shopper. So in the end we need to ensure that a cryptic score can be turned into an actionable knowledge and being transparent about our reasoning helps to do that.

Sasha Pons

Will AI technology completely take over the job of risk manager?

Chen Zamir

Technology alone will not replace the job of a risk manager. We are a service provider that supports risk managers and helps merchants reduce their total cost of fraud. Considering the complexity of the cost of fraud, it is important for us to join forces to ensure the best performance for merchants, the following chart shows how our companies work together:

	TECHNOLOGY	SERVICE
Fraugster	Artificial & Behavioural Intelligence	Chargeback Protection
ingenico ePayments	Payment Processing	Fraud Consulting

Sasha Pons

Integrating tools can take a lot of time and effort. How is Fraugster different?

Chen Zamir

Since we have already integrated into Ingenico's global online payments platform and can take advantage of the Unified Data Model used at Ingenico, merchant integration is basically effortless, only taking one click.

> **MERCHANTS SHOULD UNDERSTAND THAT THEIR DATA CAN BE USED NOT ONLY FOR SELLING THEIR PRODUCTS, BUT CAN AND SHOULD ALSO BE USED FOR IMPACTFUL PAYMENT PROCESSES.**

Sasha Pons

Can you give merchants advice on the underlying practice of building self-learning models?

Chen Zamir

To build a self learning model you want the decisions to be as accurate as possible and to do that you need data. Merchants already have the data, so that part is easy. Next you need the right infrastructure that can adjust to new information and algorithms on its own instead of a human re-training the algorithm manually. In Fraugster case, we ensure that the underlying data pool gets updated by every new transaction that is processed.
Merchants should understand that their data can be used not only for selling their products, but can and should also be used for impactful payment processes.

Sasha Pons

An essential aspect of fraud management is the concern about false positives. Are you using A/B testing to measure your performance?

Chen Zamir

A/B testing is the best practice when you are trying to determine the performance of a system. There are control groups which are small segments of populations that we pass through the system even if we flag them as high risk because it gives us a good understanding of fraud levels.
Even though A/B control groups are the best method it requires a large volume to flow through the system. Hence, The best approach but not always applicable. With manual review you take a small section of declined transactions to review manually. Looking into linked transactions, data sources, and taking the time. It is still an educated guesstimation but it's a pretty good reading. If you do manual review with a white box algorithm, then it makes the review easier and more accurate.

Sasha Pons

Thank you Chen for sharing your insights.

EXPERT BIOS

EXPERT
BIOS

Chen Zamir
is the CTO and Co-Founder of Fraugster.

Chen Zamir is the CTO and Co-Founder of Fraugster.
Chen spent more than a decade in different analytics and risk management roles including five years at PayPal in Tel Aviv.

Prior to that he was an intelligence officer with the Israeli Defence Forces. In 2013, Chen relocated with Paypal to Berlin where he began to manage the local risk team.
A year later in 2014, he teamed up with Max Laemmle (Fraugster CEO) to create Fraugster.

Today, Chen oversees the development and implementation of Fraugster's proprietary Artificial Intelligence technology and drives the company's technology vision with his team of analysts, data scientists and engineers.

EXPERT
BIOS

Sasha Pons

Is Director of Product- Fraud Prevention Solutions at Ingenico ePayments.

Sasha has spent more than 10 years working in cyber security, fraud prevention, infrastructure, privacy and compliance within international eCommerce. His expertise spans across the travel, retail, pharmaceutical and technology industries.

Sasha strongly believes that trust is the cornerstone of FinTech and being able to articulate a pragmatic and efficient cybersecurity and fraud prevention strategy is a key competitive differentiator. Because of this, his focus is on building the most data and performance driven fraud prevention platform, with the best possible UX for both Ingenico ePayments' merchants and their consumers.

Prior to joining Ingenico ePayments, Sasha worked for Booking.com. He is a French native and has lived in the Netherlands for the last four years.

ABOUT THE PARTNERSHIP

Fraugster ingenico ePayments

Ingenico Group is the global leader in seamless payment, providing smart, trusted and secure solutions to empower commerce across all channels, in-store, online and mobile.
With the world's largest payment acceptance network, they deliver secure payment solutions with a local, national and international scope. They are the trusted world-class partner for financial institutions and retailers, from small merchants to several of the world's best known global brands. Their solutions enable merchants to simplify payment and deliver their brand promise.

Fraugster is leading the future of payment security with Artificial Intelligence.
The German-Israeli payment security company is committed to boosting conversion rates while eliminating e-commerce fraud. Fraugster's proprietary AI technology combines the thought processes of human analysts with machine scalability, identifying new fraud patterns as they emerge, in real time, making it possible to detect fraud before it costs merchants damage.

Ingenico ePayments was one of the first PSPs to partner with Fraugster. With over 65,000 online businesses from all over the world relying on Ingenico ePayments they looked to Fraugster to expand its fraud detection and management capabilities with the Fraud Free Product, a new real time solution that protects merchants against online fraud. Ingenico is always on the lookout for emerging, disruptive technology companies to partner with, and Fraugster fits that profile.

www.fraugster.com
www.ingenico.com/epayments

Fraugster ingenico ePayments