Insights about E-commerce

Review of Industry & Major Threats

Nethone

Table of Contents

01 E-Commerce Industry Overview

1.1. E-commerce in numbers

1.1.1. What is e-commerce

E-commerce mostly consists of electronic transactions related to the purchase and delivery of goods and services. What can be considered an e-commerce practice:

- Retailers with online presence – "e-tailers";
- Companies selling exclusively online;
- Marketplace sellers like Amazon, eBay or Mercadolibre.

The most well-known form of e-commerce falls into the business to consumer (B2C) category, which includes online retail or online shopping.

1.1.2. Market size

E-commerce is evidently not homogenous and for this reason, estimating the real number of online merchants in the world is not a trivial mission. However, it is possible to incorporate segmentation-decision processes to avoid misclassification of websites based on the items they sell. According to Statista, in 2018:

There were **2-3 million** e-commerce companies in the world (excluding China)

1.8 billion people worldwide purchased goods online

Global e-retail sales amounted to **$2.8 trillion**

1.1.3. Top selling industries

Interestingly, **fashion** is the top selling industry in almost all **countries** with **clothing**[1] being the **highest** contributing **product category.** The increase in demand in the fashion industry in the online world **owes itself mainly to the improvement in returns policies**[2]. Following clothing, shoes and consumer electronics are the 2nd and 3rd most popular categories, respectively.

1	Clothing
2	Shoes
3	Consumer electronics
4	Books, movies & music
5	Cosmetics & body care
6	Bags & accessories
7	Food & drinks
8	Household appliances
9	Furniture & household goods
10	Sports & outdoor

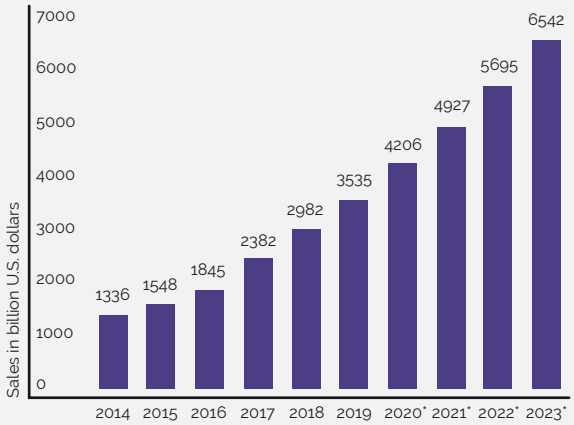
Source: Statista

1.1.4. An on-growing industry

Consistent with eMarketer and Statista, in 2019 global e-commerce sales were expected to rise **20.7% to $3.5 trillion**. As the chart shows, by 2021 this index will be landing close to $5 trillion.

Asia-Pacific and Latin America will be the two regions with highest year-on-year growth rates. Yet, Western Europe owns three of the top six e-commerce markets, led by **UK, Germany and France**.

Retail e-commerce sales worldwide from 2014 to 2023 (in billion U.S. dollars)



*Forecast includes products or services ordered using the internet or via any device, regardless the payment method and excluding travel and event tickets.

Source: Statista

[1] Retrieved from Statista

[2] Retrieved from Pipe Candy

1.2. Mobile commerce

Over time, mobile shopping has gained a tremendous share of the global e-commerce market: customers are increasingly using their mobile devices for various online shopping activities. The industries that are mostly affected by the growth of m-commerce are financial services including mobile banking, telecommunication, retail and information services.

1.2.1. Types of m-commerce

Mobile Shopping. Allows a customer to purchase from a mobile device using a marketplace application such as Amazon or through a web app.

Mobile Banking. Enables customers to conduct fanatical transactions like bank transfers. Usually done though secure, dedicated app provided by the financial institution.

Mobile Payments. Enables users to buy products in person through digital wallets such as Apple Pay, Android Pay and Samsung Pay.

1.2.2. The boom

Mobile retail commerce as percentage of retail e-commerce

2018	2019	2020	2021
63.5%	67.2%	70.4%	72.9%

In Q4 2018, desktop PCs accounted for approximately the same amount of global e-retail orders as smartphones. However, smartphones were the number one device in terms of retail website visits in 2018. This can be explained by the intense demand during the Christmas holiday season.

Source: Statista

1.2.3. Undercover secret of m-commerce

There are various reasons that explain why this type of online commerce is growing at such a fast pace.

1. Firstly, these devices **enhance costumer flexibility:** e-commerce already enables access to a wider range of products and competitive prices; with mobile commerce, these features are subject to an increased flexibility of spaces for device usage. For this reason, m-commerce is sometimes referred to as "contextual commerce" – listing products where customers are spending most of their time.
2. On top of these bright benefits, there is also a **variety of payment options**, most common being Apple Pay, PayPal One-Touch, Visa Checkout and Amazon Pay.
3. Ultimately, online merchants using the mobile channel have registered **higher conversion rates and ROI.**

> As long as they have a mobile device, they can shop whenever they want, wherever they want.

02 The Dark Side of E-commerce

2.1. Introduction to payment methods

The vast diversity of payment methods is in fact one of the key drivers of the online commerce growth. As so, these two industries go hand in hand and together they are exposed to similar market risks.

The most common payment methods used in e-commerce are credit cards, mobile payments, bank transfers and e-wallets, followed by those less popular such as prepaid cards, direct deposit and cash[4].

In m-commerce, the most used methods, are mobile wallets, contactless mobile payments, closed loop mobile payments, money transfers, mobile point-of-sale and carrier payments[5].

2.2. Cybercrimes

Unfortunately, the consequences of the dimension and growth potential of e-commerce are not only positive. Fraudsters can't resist taking advantage, and online payment fraud is rising fast. The most common cybercrimes are:

Card Not Present Fraud

Unauthorized use of payment card while purchasing goods and services online or via telephone. Stolen data includes cardholder's name, billing address, account number, three digit security code and the expiration date. According to Juniper Research, in Europe, 60% of card fraud are associated with CNP transactions.

Account Takeover

Commonly known as "stolen identity", ATO occurs when a criminal gets a hold on one's information, such as usernames, email addresses, passwords and social security numbers. With this they are able to provide proof of their identity since they possess one's personal details.

[4] Retrieved from PaymentWall: Payment Service Provider

[5] Retrieved from BigCommerce: SaaS E-commerce Platform

2.3. How it works

Hacker steals card/personal details to later sell/buy it on the dark web to/from fraudsters

1

Fraudster uses the stolen information to buy things online

2

Merchant validates transaction and ships the good to the fraudster

3

Cardholder detects the fraudulent transaction and contacts his/her bank

4

Cardholder's bank contacts the merchant to report the incident

5

Merchant receives a charge-back notification from the cardholder's bank

6

2.4. Merchant's liability to fraud

Cyber payments lack the standard security measures that **Card Present** transactions secure. Since this risk is higher, the merchant is liable for the acceptance of any fraudulent order and incur into losses like:

Value of the product/service sold - Original fraudulent shipment;
Refund the scammed customer - Chargeback fee issued by the cardholder's bank;
Penalty from acquiring bank - Merchant's bank may charge a fee for every chargeback received and increase this fee as the volume of fraudulent transactions goes up and so does the number of chargebacks;
Customer experience - If by mistake the merchant rejects a legitimate customer there is a high risk that the loss of such customer will not be only one-time, but rather a loss of their lifetime shopping potential;
Manual reviews – Costs associated with time spent reviewing orders. Delaying an order might decrease the chances of future purchases by that client.

2.5. Dimension of the problem

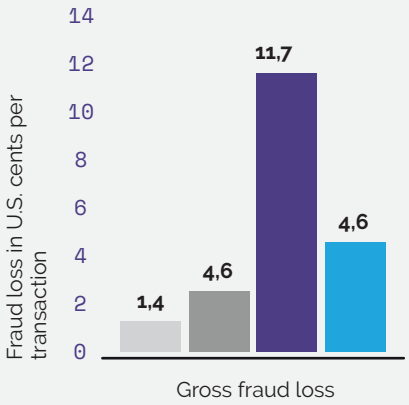
Retrospective | Prospective

- Merchants' total fraud costs as a percentage of revenue went from 7.6% in **2016** to 8% in **2017**[6].
- In **2018**, 82% of organizations reported problems related to payment fraud; Large organizations were particularly vulnerable as business with over $1 billion revenue registered a jump of 7% (from 80% to 87%)[7].
- In **2019**, 42% of organizations experienced loss as a result of payment fraud; There was a particular increase in fraud criminality in Automated Clearing House (ACH) Fraud* via:
  1. Debits (2018: 28% 2019: 33%)
  2. Credits (2018: 13% 2019: 20%)[7]

[6] Retrieved from Javelin Strategy & Research
[7] Retrieved from Association for Financial Professionals Payments Fraud & Control Survey
*ACH Fraud – ACH is a tool used by financial institutions to handle direct deposits, checks or bill payments between businesses and individuals; Through phishing, fraudsters obtain a checking account number and a bank routing number which they then use to steal bank account passwords.

Payment fraud is a persistent problem that is only getting worse despite repeated warnings and educational outreach.

Fraud loss per card payment transaction in USA 2018 - by transaction



CP with PIN
CP with signature or no CVM*
CNP*
Overall

In the United States, **Card Not Present fraud** is the type of fraud with the biggest impact for the merchants, which translates into a gross loss of **$11.7 cents** per transaction in 2018.

Retrospective

Prospective

- As statistics have been showing, the growth of fraud is and will continue to be driven by the rapid expansion of the e-commerce market, higher money flows in the online channel and the increased use of mobile payments.

2.6. How do fraudsters profile merchants?

Luxury goods & services

VODs & streaming services

Subscriptions (e.g. possibility of testing cards)

2.7. Why are fraudsters focusing on m-commerce?

- Mobile devices, especially iPhones, present very similar characteristics - installed software and plugins, graphical and screen settings - and are therefore much harder to be distinguished from each other.
- Mobiles are robust against device fingerprinting.
- Old phones are cheaper and more difficult to track.

03 Geographies

3.1. Statistics

	Brasil	UK	USA
Total population	**211.4M**	**67.6M**	**329.1M**
Internet penetration	**68%**	**87%**	**94%**
Mobile penetration	**97%**	**72%**	**82%**
Online shoppers	**60M**	**48M**	**191M**
E-commerce revenue	**USD 15.3B**	**USD 720.8B**	**USD 547.7B**

*All numbers as of 2018 and 2019

3.2. Facts

Brazil

Brazil is the largest e-commerce market in Latin America, ranked 10th in the world for its sales. The most important players are B2W Digital, MercadoLivre and Alibaba. Preferred payment methods are credit cards and Boleto Bancário. The most common types of fraud are directly related to credit cards – the levels are among the highest in the world.

United Kingdom

The United Kingdom takes the lead of online shopping penetration in Europe and is the third largest in the world. The leading multichannel retailers in 2019 are the fashion retailer New Look, Schuh and Argos. MasterCard holds the largest share of payments. The most common type of fraud is CNP. By 2021, 93% of the country's online users will purchase goods/services online.

USA

The world's most developed market by far, the United States of America is the global standard for e-commerce. The top American e-commerce platform are Macy's, Wish and Lowe's. Visa is the preferred payment method. As e-commerce and mobile commerce present impressive growth rates, the country sees more than half of all global payment card fraud.

04 How to Prevent Fraud in Online Payments

4.1. Payments are changing

Timeline

2001

Traditionally, card payments usually required two steps: **Authorization** – when cardholder's bank approves the payment; **Capture** – when the card is charged.

Here's how it works:

Despite all efforts in security and verification systems, debit and credit card payments had still a major exposure to fraud risk. To tackle this problem, card networks implemented the first version of what it's known to be **Authentication**, through a system called 3D Secure 1.

3DS 1

Customer inputs card details to confirm a payment

Customer is redirected to a page where bank asks for a code of password to approve the purchase

Some famous examples of branded 3DS 1 are Visa Secure, Mastercard Identity Check or American Express SafeKey.

Advantages of 3DS1 for the Merchant:

- Building an extra layer of fraud protection.
- Ensuring that only legitimate users follow through the pipeline.

- Shifting liability for chargebacks from merchants to the customer's bank.

Disadvantages of 3DS1 for the Merchant

- Adding a step to the payment can add friction to the checkout flow and lead customers to abandon the purchase.
- Some banks require from their cardholders to remember passwords to complete authentication, which can be easily forgotten and lead to higher rates of cart abandonment.

4.2. An eye over European payments

October 8,
2015

In order to better protect consumers when they pay online, promote the use of innovative online and mobile payments and make cross-border European payment services safer, the European Parliament adopted a legislation: **The 2nd Payment Services Directive (PSD2)**.

The most important regulatory requirement from this directive is the need for **Strong Customer Authentication (SCA)** on the majority of online payments, with the goal of reducing fraud and make online payments more secure.

With SCA, a new form of authentication is employed – **3DS2** - which is mandatory whenever a payment isn't eligible for exemption* or when the bank denies an exemption request.

Like 3DS1, 3DS2 occurs at the very beginning of the transaction. This time, the customer must respond to a two-factor authentication prompt issued by their bank. This can be in the form of:

* Payments such as fixed-amount subscriptions, phone sales, merchant-initiated transaction or general low-risk transactions, can be exempt from SCA.

Something the customer knows	Something the customer has	Something the customer is
(Password/PIN)	(Hardware)	(Fingerprint)

In order for the payment to go through, the transaction should have at least two of these elements verified. Without it, many payments may be declined by the bank of the merchant's client. Addionally, for authentication to happen, the customer should be on the merchant's website or mobile app.

Advantages of 3DS2 for the Merchant: "Frictionless Authentication"

- The merchant and their PSP are able to send more data elements to the cardholder's bank, easing the process of making a decision about a transaction.
- Automatic requests for eligible exemptions enable the bank to assess a transaction before the prompt is sent to the customer, avoiding friction and abandonment chances.

September 14, 2019

PSD2 went into effect!

December 31, 2020

Requirements are expected to be fully enforced.

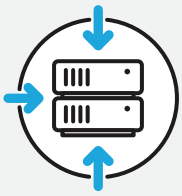
05 Our Solution

At Nethone, we are passionate about helping merchants resolving their fraud problems. We have developed proprietary **AI-driven Know Your Users analytical system** that helps convert threats into well-informed and profitable decisions.

Our innovative cloud-based solution - Nethone Guard is based on 4 pillars:

Nethone Guard

Exhaustive user profiling data



Seamless data hub

Thoroughly tested Machine Learning

Human ingenuity at your disposal

Nethone Guard was designed to detect payment fraud by identifying anonymisation, automation, and anomalous behaviour. Profiler is a proprietary solution that gathers over 5,000 attributes and unique fingerprints about each user or device used to access a website. This extensive set of attributes ranges from:

Hardware, Software and Browser Intelligence

E.g. GPU characteristics, GPU detection, virtual machine detection, number of processor cores, mobile device detection

Behavioral Data

E.g. Mouse/touchpad movements, swipes, keystroke dynamics, gyro readings, accelerometer, clipboard usage

Network Intelligence

E.g. IP geolocation, TCP/IP stack analysis, connection type detection (Wi-Fi, cellular), OS fingerprinting, VPN/Proxy/Tunneling detection, Tor detection, public IP leak

To analyse the data gathered through the whole user flow, we use advanced Machine Learning (ML) algorithms. Attributes are analysed by our AI models to find non-obvious links between them. Our profiler and models are carefully deployed and enriched by the Data Scientist (DS) team within Nethone, working closely with our clients. They assist whenever the merchant considers necessary and work on constant optimisation of the models in order to make sure all key KPI of the client are met.

> ML has proven to be more effective than other statistical rules with proficiency to analyse highly unstructured data.

06 References

https://searchmobilecomputing.techtarget.com/definition/m-commerce

https://www.jpmorgan.com/merchant-services/insights/reports/european-overview

https://www.merchantriskcouncil.org/resource-center/whitepapers/2017/the-future-of-digital-payments-in-europe

https://beeketing.com/blog/future-ecommerce-2019/

http://blog.paymentwall.com/guides/types-of-payment-methods-for-ecommerce

https://www.bigcommerce.com/blog/mobile-commerce/#why-does-mobile-commerce-matter

https://www.signifyd.com/resources/fraud-101/why-liable/

https://www.experian.com/assets/decision-analytics/reports/global-fraud-report-2018.pdf

http://blog.pipecandy.com/e-commerce-companies-market-size/

https://www.emarketer.com/content/uk-ecommerce-2019

https://fesrvsd.fe.unl.pt:2058/topics/871/online-shopping/

https://www.prnewswire.com/news-releases/payments-fraud-jumps-to-record-high-82-of-businesses-impacted-survey-finds-300825669.html

https://s3.amazonaws.com/dive_static/paychek/Financial_Impact_of_Fraud_Study_FINAL.pdf

https://www.thepaypers.com/

https://disfold.com/top-e-commerce-sites-us/

https://www.investopedia.com/terms/c/cardnotpresent-fraud.asp

https://www.onespan.com/blog/top-account-takeover-fraud-schemes-and-how-protect-against-them

https://en.wikipedia.org/wiki/Payment_Services_Directive#Revised_Directive_on_Payment_Services_(PSD2)

https://stripe.com/en-pl/guides/sca-payment-flows