PUBLISHED: SEPTEMBER 2023

THE AGE OF CYBERCRIME

CYBERSECURITY AND PAYMENT FRAUD IN THE PAYMENT ECOSYSTEM

INTRODUCTION

One of the hottest topics in the post-pandemic period has been the evolutionary leap in digitization and how it has changed our daily lives. In addition to the many advancements caused by digitization, there is also a negative aspect that deserves more attention: the marked increase in cybercrime and payment fraud.

With much of our daily lives and routines moved online during the pandemic, cybercriminals are using increasingly advanced and effective tools to find vulnerabilities in the digital ecosystem. There were more security breaches in 2020 than in the last 15 years combined and that number rose an additional 17% in 2021.

We need a united effort across the region to fight fraudsters and hackers since individual organizations have only a limited view of the threats. Cooperation and partnerships enable us to find the most efficient ways to fight cybercrime as a collective.

At Mastercard, we work every day to be at the forefront of cyber defense to help all industry stakeholders and provide the effective solutions needed to prevent cyber-attacks and payment fraud.

Although we see more and more risk factors emerge every day, I am more optimistic than ever that together we can revolutionize the field of data protection.

The purpose of this white paper is to provide an overview of the current threats, identify the key challenges in cyber-security and fraud protection, describe how to manage and prevent these attacks, and explain how Mastercard's diverse solutions can take the burden off your shoulders so you can focus on digital developments and innovations.

I hope this paper adds to the discussions about cyber-security in your organization. If you have any questions or feedback, we look forward to talking with you.

Sincerely,
PAOLO BATTISTON
Executive Vice President, Services, Europe

ANTHROPOLOGICAL OVERVIEW

INTRODUCING THE HOMO DIGITALIS

The Homo Digitalis, or the digital-age human, navigates comfortably in their everyday lives with modern technology. Although they use online tools, they don't fully understand how they work. They fail to perceive the lurking dangers and panic when trouble arises. Many mistakenly believe that the solution lies in disconnecting from the digital world, yet the inevitability of digitalization and technological advancement must be emphasized.

Global, well-equipped hacker armies launch attacks on the digital realm. In general the Homo Digitalis is much more vulnerable to these attacks due to their lack of comprehension of technological threats. Homo Digitalis seeks refuge in offline existence, unaware that digital development cannot be avoided. Enterprises require mostly invisible but well-prepared partners capable of protecting them from hacker attacks.

These defense experts can identify attacks and effectively respond to the challenges posed by cybercriminals. They are the hidden guardians of the digital world, providing defense against the growing onslaught of cyberattacks for the homo digitalis groups.

CYBERCRIMINALS ARE CHANGING STRATEGY.

ARE YOU KEEPING UP?

Digitization is an irreversible process that will only continue to advance, consequently **INCREASING THE VULNERABILITY OF HOMO DIGITALIS.** In this world, **BEING A HACKER IS CHEAP.** Affordable, high-tech solutions are within reach for everyone. At the same time, the complexity of the digital world is increasing constantly, resulting in **MORE AND MORE POTENTIAL THREATS,** requiring new protective measures. Hackers are always looking for new **WEAK LINKS:** the latest trends suggest these are now the **HUMANS** using systems, and **SUPPLIERS.**

The key players in prevention are companies – if they are mindful and sufficiently prepared, their systems will be secure against global attacks, including large-scale ones.

THE AIM OF THIS REPORT IS TO SHOWCASE THE WAYS CYBERCRIMINALS EXPLOIT SUCH WEAKNESSES, AND OFFERS SUGGESTIONS TO DEFEND AGAINST THEM.

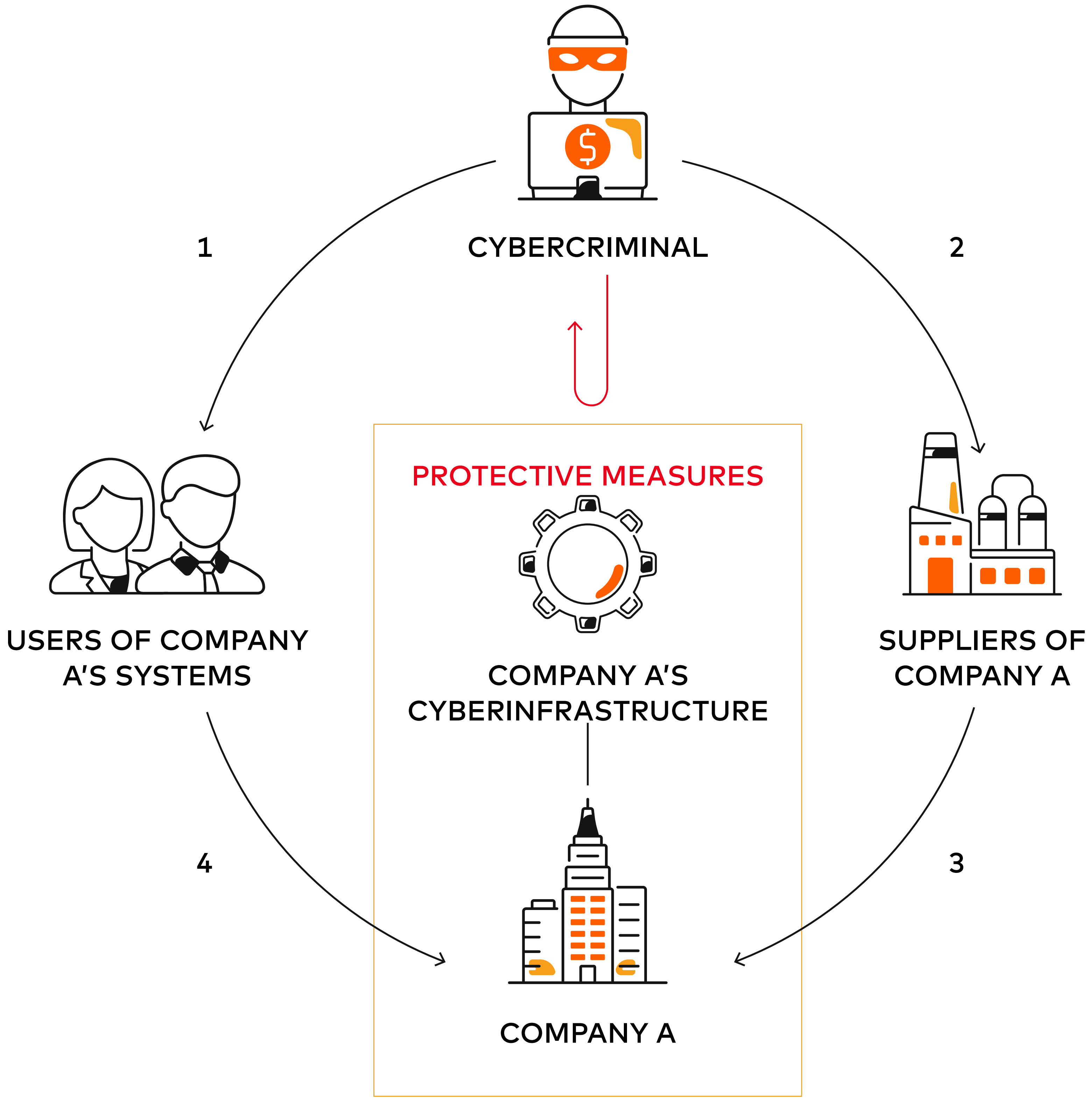
The report was prepared using a number of studies, including ones by the ECB, MNB, interviews with industry experts, and **LEVERAGING MASTERCARD'S OWN CYBERSECURITY SOLUTIONS,** offering global coverage.

THE NEW STRATEGY IS ABOUT

TARGETING

THE NEW WEAK LINKS

CYBERCRIMINALS ARE ALWAYS LOOKING FOR THE WEAK LINKS. AS MORE AND MORE PROTECTIVE MEASURES ENSURE THE SAFETY OF COMPANIES' INFRASTRUCTURE, HACKERS ARE TURNING TO ATTACKS AIMED AT THE HOMO DIGITALIS, AND THE SUPPLY CHAIN.



1 Nowadays, if a cybercriminal wants to attack Company A, most likely they will face a difficult task: **COMPANIES STRONGLY PROTECT THEIR CYBERINFRASTRUCTURE.**

2 However, the cybercriminal still has 2 ways to go: Towards **USERS OF COMPANY A'S SYSTEMS**, and **SUPPLIERS** of Company A.

3 If **SUPPLIERS** of Company A do not have **SUFFICIENT CYBERSECURITY MEASURES** in place, and do not comply with regulations, such as **DORA OR NIS2** in the near future, Company A is in danger.

4 With infrastructure protected, cybercriminals are searching for other **WEAK LINKS**, one of which is the **HUMAN ELEMENT, THE HOMO DIGITALIS**. This can be exploited through **SOCIAL ENGINEERING**.

AGENDA

CHAPTER 1

CYBERCRIME AND SECURITY

OVERVIEW OF CYBERCRIME IN EUROPE AND HUNGARY

ADDRESSING THE KEY CHALLENGES OF CYBERSECURITY

CHAPTER 2

PAYMENT FRAUD

OVERVIEW OF PAYMENT FRAUD IN EUROPE AND HUNGARY

ADDRESSING THE CHALLENGES OF PAYMENT FRAUD

CYBERCRIME & SECURITY

CHAPTER 1

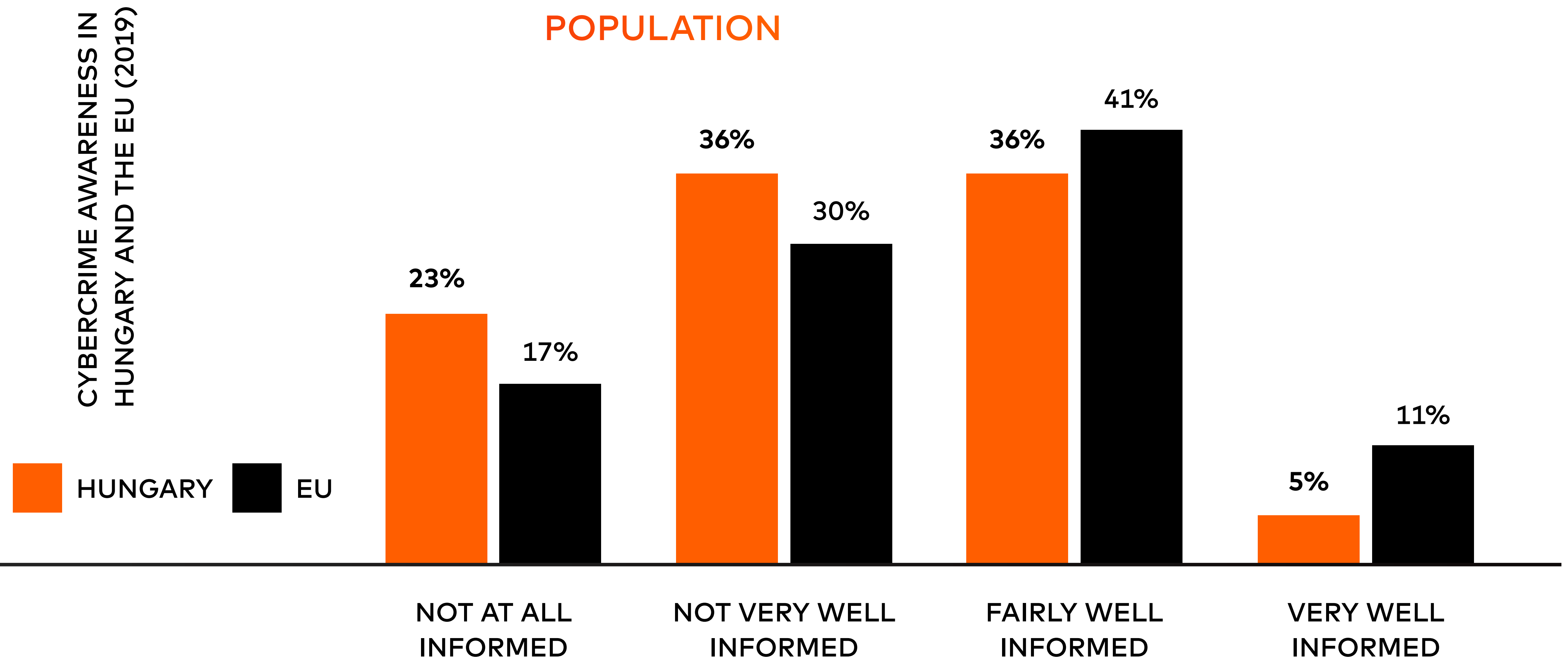
OVERVIEW OF CYBERCRIME IN

EUROPE AND HUNGARY

HUNGARY FACING GROWING RISK

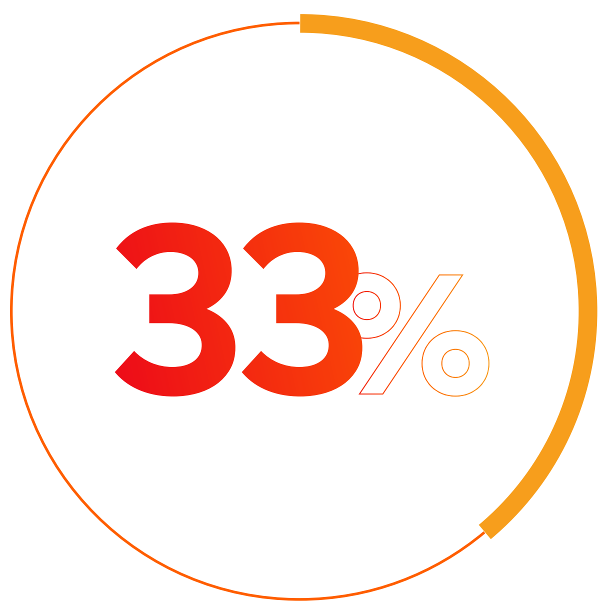
CYBERCRIME AWARENESS IS LOW

AMONG THE HUNGARIAN POPULATION

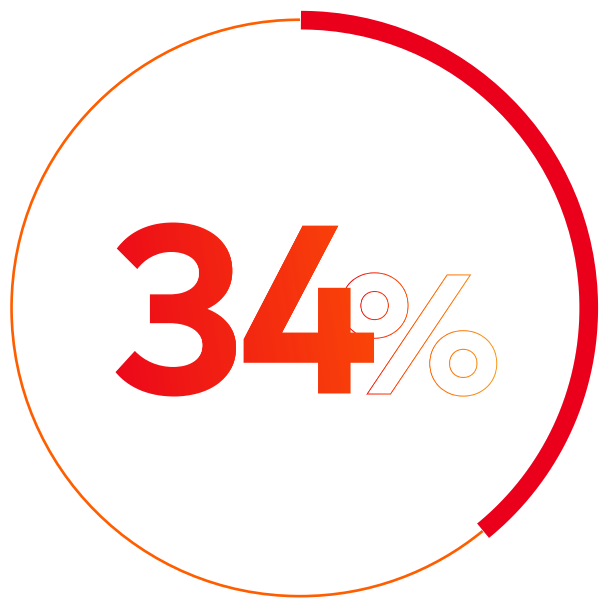


The number of attempted and successful cyberattacks, such as data breaches, is on the rise, **YET MORE THAN HALF OF HUNGARIANS ARE NOT WELL-INFORMED ABOUT CYBERCRIME RISKS,** which is markedly below the EU average. In Hungary, almost one in four people have no information or knowledge of cybercrimes, and only 5% report being very well-informed on such matters. The awareness in the European Union is significantly higher, indicating that **HUNGARY HAS SIGNIFICANT ROOM FOR IMPROVEMENT IN EDUCATING USERS ABOUT CYBERSECURITY.**

In addition to low cybercrime awareness, **MOST HUNGARIANS SAY THEY WOULD NOT REPORT CYBERCRIME:** only about one in three Hungarians would report that their personal data was stolen or that they were a victim of online banking fraud. The lack of general knowledge about cybercrime coupled with a low willingness to report data theft and fraud makes local customers more vulnerable to cybercriminals. This phenomenon reflects to the mindset of Homo Digitalis: even though it utilizes the necessary tools, it anticipates third-party protection.



OF HUNGARIANS WOULD NOT REPORT PERSONAL DATA THEFT*

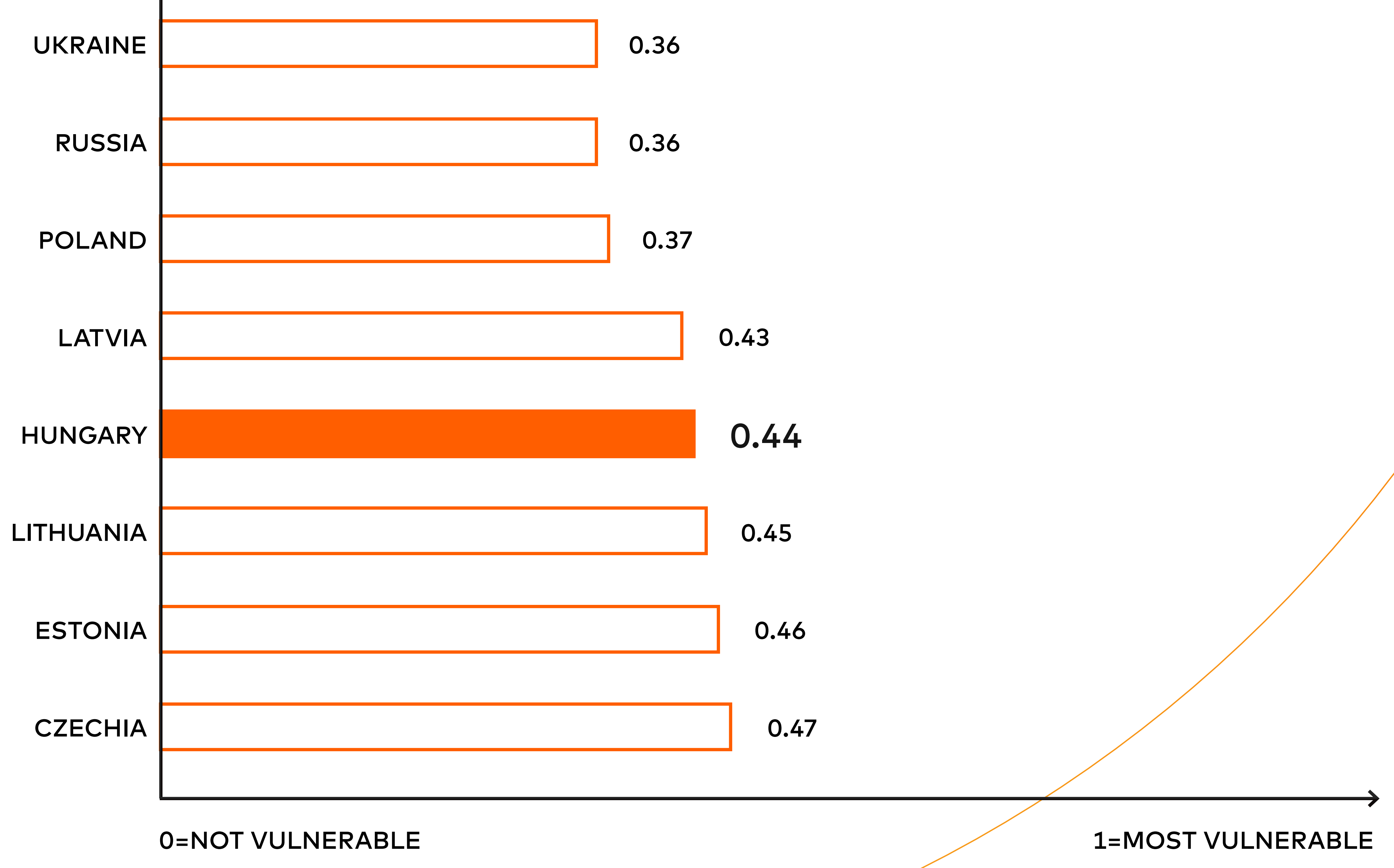


OF HUNGARIANS WOULD NOT REPORT ONLINE BANKING FRAUD*

Sources: Profilics Testing

CYBER RISK

IS ON OUR DOORSTEP: THE CORRELATION BETWEEN CYBER RISK, WAGES AND THE TIME WE SPENT ONLINE



CYBER RISK INDEX IN CEE COUNTRIES (2020)

HUNGARY HAS THE FOURTH HIGHEST EXPOSURE RATE AMONG COUNTRIES IN THE CENTRAL AND EASTERN EUROPE REGION AND FACES MODERATE CYBER RISK.

High-income countries with more advanced technological infrastructure face a higher risk of cybercrime, as the most important factors are:

TIME SPENT ONLINE

with greater exposure to threats of cybercrime

HUNGARIANS SPEND 1-2 HOURS A DAY ONLINE ON AVERAGE.

HIGHER WAGES

offering cybercriminals the potential for larger financial gains

Notes: The Cyber Risk Index *(CRI)* predicts the risk of becoming a victim of cybercrime based on the country of residence, with a score of 0 corresponding to no cyber risk and a score of 1 corresponding to maximum cyber risk. The CRI is composed of 14 indicators that contribute to country-level cybercrime, categorized into socio-economic-, digital-, cyber-, and crime-related factors.Sources: NordVPN and Statista 2020 CRI Survey

CLIENTS' PERSONAL AND FINANCIAL INFORMATION ARE THE MOST ATTRACTIVE TARGETS FOR CYBERCRIMINALS

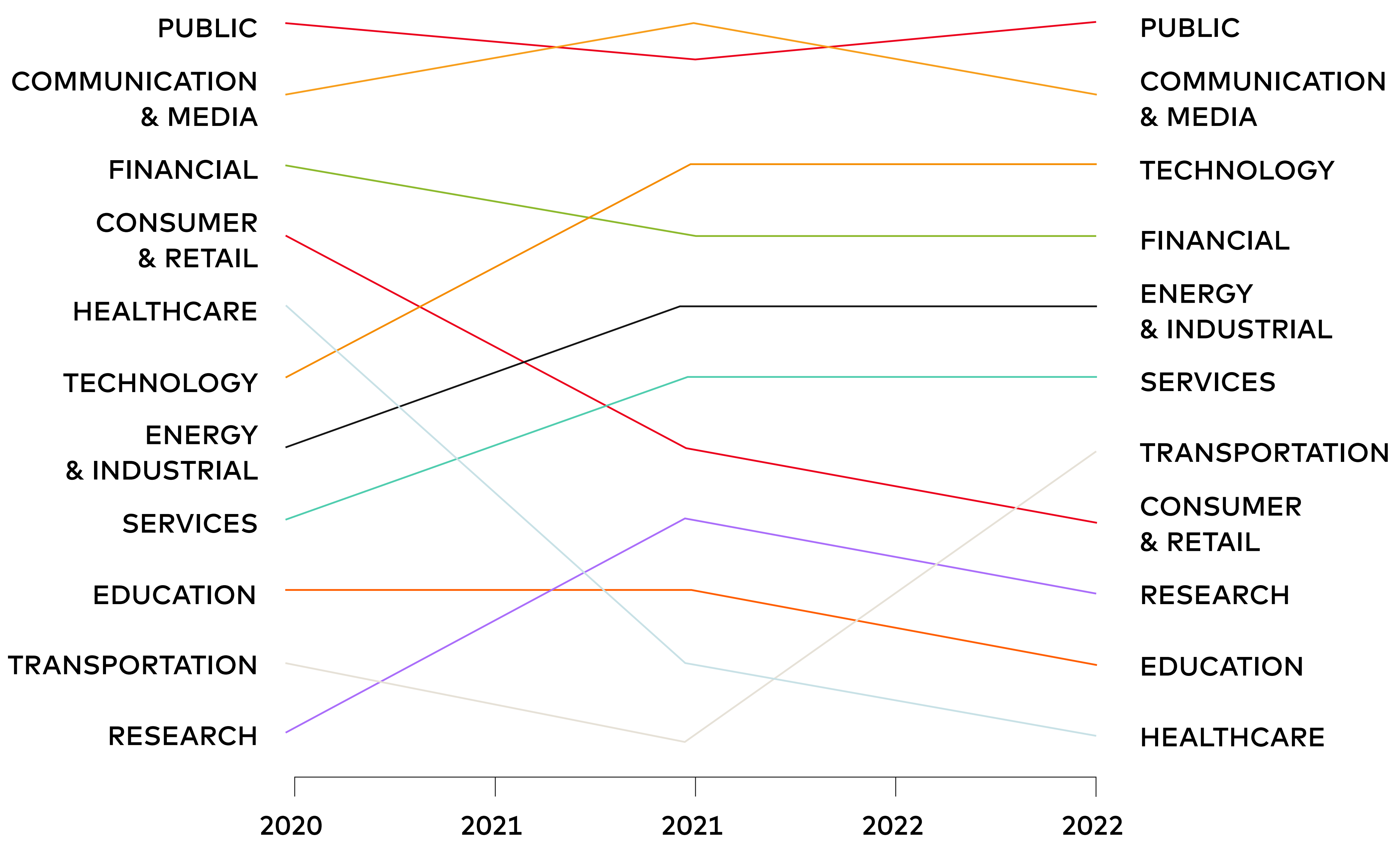
WHICH INDUSTRIES FACE THE MOST RISK?

To gather personal and financial information, cyberattacks mostly targeted **THE PUBLIC AND FINANCIAL SECTORS** and **THE COMMUNICATION & MEDIA INDUSTRY** in Hungary.

2021 saw a rise in the importance of **THE TECHNOLOGY, ENERGY & INDUSTRIAL AND SERVICES** sectors, complemented by **TRANSPORTATION** during 2022, whereas the Consumer & Retail and Healthcare industries dropped in the rankings.

CYBER ATTACKS IN HUNGARY

TOP ATTACK METHOD	47%	of attacks in Hungary occurred through malware
TOP ASSET AT RISK	26%	of cyberattacks in Hungary target client personal and financial information
TOP THREAT ACTOR	48%	of attackers in Hungary are financially motivated



INDUSTRIES WITH THE MOST CYBERATTACKS IN HUNGARY

Sources: Mastercard Cyber Quant platform: Data gathered from 14 data sources including: Mastercard threat intelligence, cybersecurity event reports, dark web websites, hacker forums, RSS feeds

THE EFFECT OF THE UKRAINE WAR ON HUNGARY'S CYBERWARFARE

WHICH ASSET TYPES FACE THE MOST RISK?

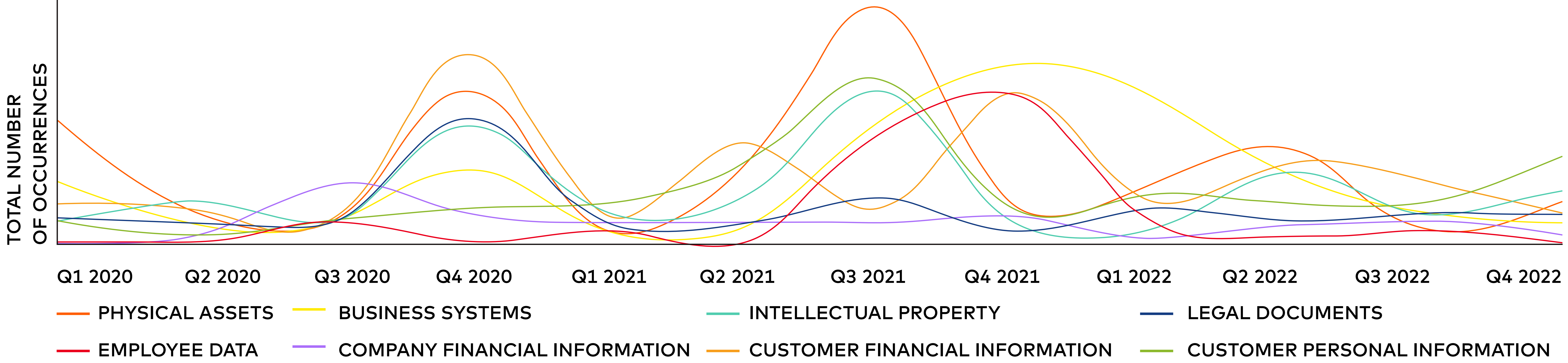
Despite regulations protecting personal data in Europe, **ATTACKS ON PERSONAL INFORMATION SIGNIFICANTLY INCREASED** in Q3 2021. After a period of lower activity, **SPIKED AGAIN IN Q4 2022,** potentially driven by the increasing number of **SCAMS,** such as phone calls and fake websites pretending to be financial institutions and courier companies, among others.

The pattern of attacks targeting **PHYSICAL ASSETS AND BUSINESS SYSTEMS** may indicate that the attackers' goal is continuous disruption of business-critical and operational systems.

According to our data, Hungary's cyberattack rate in 2022 decreased, potentially influenced by the Ukraine conflict redirecting cybercriminal activities.

ONE OF THE LARGEST CYBERATTACKS

In 2020 the international DDoS[1] attacks mainly targeted financial institutions but also reached Hungary's largest telecommunications provider, with the volume and complexity of the attacks causing temporary outages.



MOST COMMON TYPES OF CYBERATTACKS IN HUNGARY

Sources: Mastercard Cyber Quant platform
Reuters.com, Mastercard Cyber Quant platform: Data gathered from 14 data sources including: Mastercard threat intelligence, cybersecurity event reports, dark web websites, hacker forums, RSS feeds

[1] DDOS (Distributed denial of service) attacks aims to force a computer system offline by flooding it with data from multiple computers at the same time

TARGETING

THE HOMO DIGITALIS: EMAIL SOCIAL ENGINEERING IS ON THE RISE

WHAT ARE THE MOST COMMON TYPES OF CYBERATTACKS THREATENING THE HOMO DIGITALIS COMMUNITY?

MALWARE

Malware or malicious software performs undesirable operations such as data theft or other types of computer compromise. Main types of malware include trojans, viruses, worms and spyware.

EMAIL SOCIAL ENGINEERING

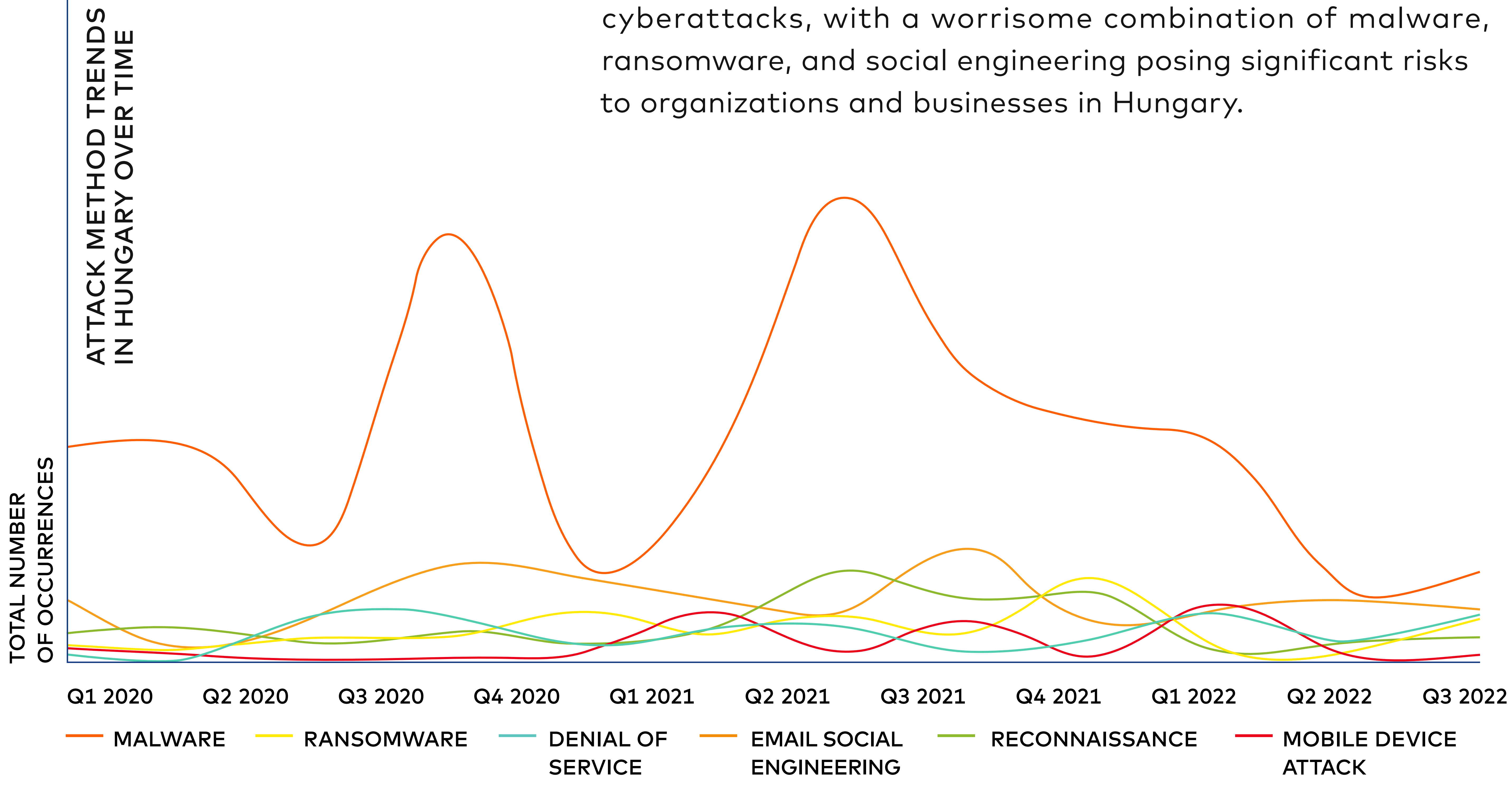
Email social engineering is a communication in which an adversary manipulates and exploits people using emails, including spam, scams, phishing and/or spear-phishing.

RANSOMWARE

Ransomware is a type of malware *(like viruses, trojans, etc.)* that infects users' computer systems and manipulates the infected system so the victim cannot access their data.

Malware emerged as the predominant attack type in Hungary, accounting for nearly half of all attacks between 2020 and 2022.

It closely followed by email social engineering, highlighting the vulnerability of homo digitalis and prime target of cyberattacks, with a worrisome combination of malware, ransomware, and social engineering posing significant risks to organizations and businesses in Hungary.



ATTACK METHOD TRENDS IN HUNGARY OVER TIME

Sources: Mastercard Cyber Quant platforms; Ipsos
Mastercard Cyber Quant platform: Data gathered from 14 data sources including: Mastercard threat intelligence, cybersecurity event reports, dark web websites, hacker forums, RSS feeds

ADDRESSING THE KEY CHALLENGES OF CYBERSECURITY

GOVERNMENTS, ORGANIZATIONS, AND CORPORATIONS STAND AT THE FOREFRONT OF CYBERATTACKS

PREVENTING CYBERATTACKS: ESSENTIAL TOUCHPOINTS

KEEPING SECURITY SYSTEMS UP TO DATE

ENSURING THAT SUPPLIERS ARE ALSO PROTECTED

ALWAYS STAY VIGILANT- ZERO TRUST POLICY

BETTER UNDERSTANDING CYBERSECURITY RISK EXPOSURE

Source(s): Mastercard Advisors Analysis

CYBERSECURITY CHALLENGES:

KEEPING SECURITY SYSTEMS UP TO DATE

As IT systems becoming more complex, fraudsters are becoming more sophisticated and versatile in their methods as well.

HOW DOES IT HAPPEN?

- Cyberattacks or data breaches may arise through technical methods or human errors, whether malicious or non-malicious.

WHAT YOU SHOULD DO?

- Keep all your security systems up to date.
- Have a clear picture of the security of the IT systems and to identify vulnerabilities.
- Educate your workforce regarding cybersecurity.

HOW TO TAKE ACTION?

- To safeguard data that is stored electronically, data management services are vital, coupled with more focused regulatory efforts.
- For example, DORA*, sets risk management thresholds for organizations to guard against and mitigate cyberattacks.

REGULATORY EFFORTS CAN ALSO HELP RAISE SECURITY STANDARDS collectively by imposing minimum IT security requirements.
The EU's proposed digital finance package, the **DIGITAL OPERATIONAL RESILIENCE ACT (DORA),** is the operational resilience framework for the financial sector. It sets uniform requirements for the security of network and information systems of companies and organizations operating in the financial sector as well as critical third parties which provide ICT-related services to them.

Source(s): EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)

CYBERSECURITY CHALLENGES:

ENSURING THAT SUPPLIERS ARE ALSO PROTECTED

HOW DOES IT HAPPEN?

- Through outsourcing data, entities lose the trusted shield provided by their own secure IT systems. Hackers identify the weakest spots in the cybersecurity chain, making it vital to consider the security of the entire ecosystem.

WHAT YOU SHOULD DO?

- Organizations need to implement solutions that can monitor the fraud exposure of their supply chain, with the support of regulatory bodies, similar to the UK's National Cyber Security Centre.

HOW TO TAKE ACTION?

- Constant monitoring - every other company in the value chain should be protected against cybercrime.

54%

of organizations experienced a **DATA BREACH** in the past 12 months **CAUSED BY A BREACH IN A COMPANY IN THEIR SUPPLY CHAIN**

"Having a house with a top-notch security system and alarms means nothing if the neighbor has a spare key and loses it. It is the same with IT security – criminals are heading towards the smallest resistance, so you need to make sure the supply chain is protected as well."

TAMÁS MARSI
Lead of Event Detection Team
National CyberSecurity Center

Source(s): Mastercard Advisors Analysis; digital-operational-resilience-act.com; Ponemon Institute

CYBERSECURITY CHALLENGES:

ALWAYS STAY VIGILANT:

ZERO TRUST POLICY

HOW DOES IT HAPPEN?

- **USERS NEED TO BE ABLE TO WORK FROM ANYWHERE** and access the organization's systems securely, while devices and data should be well protected against cybercrime. The bottom line: organizations must remove inherent trust from the network.

WHAT YOU SHOULD DO?

- Organizations first need to **ASSESS HOW USERS INTERACT WITH THEIR DIGITAL DEVICES.**
- Use zero trust security policies are based on the **LEAST-PRIVILEGED ACCESS MODEL**. They grant users 'just-enough access' to do their jobs and authenticate them continuously based on their identities and roles, regardless of their location.

HOW TO TAKE ACTION?

- Always **AUTHENTICATE USERS AND CONTROL THEIR ACCESS TO DATA AND SERVICES** according to the east-privileged principle.
- Monitor the health of enterprise services and devices
- Set policies and control access according to the value of the respective service or data.
- Never trust networks, not even local ones.

AUTHENTICATE EVERY USER

VALIDATE ALL DEVICES

LIMIT DATA ACCESS

Source(s): Mastercard Advisors Analysis

CYBERSECURITY CHALLENGES:

BETTER UNDERSTAND CYBERSECURITY

RISK EXPOSURE

HOW DOES IT HAPPEN?

- There is often a gap between a firm's perceived risk of cybercrime and the actual risk. As a result, their focus may shift from IT security to other matters, leaving the system vulnerable to hackers. This lack of awareness can prevent leaders from making appropriate and sufficient investments in cybersecurity.

WHAT YOU SHOULD DO?

- To prevent cyberattacks, organizations should have a clear understanding of the data they possess. This enables them to assess potential cybersecurity risks and identify weaknesses in their systems. By doing that they can prioritize their investments in IT security more effectively.

HOW TO TAKE ACTION?

- Organizations should undertake a **THOROUGH ASSESSMENT OF THEIR CYBER RISK EXPOSURE,** identify the monetary and non-monetary losses they might incur from an attack, and **INVEST STRATEGICALLY TO IMPROVE THEIR CYBER-SECURITY** where it will have the greatest impact.

"Although there has been progress in recent years, it is a great challenge to explain the cyber risk to SMEs and bigger organizations. We need to make sure that IT security becomes a part of the organizational culture. One way is to help leaders understand their companies' risk exposure, so they take this matter more seriously."

TAMÁS MARSI
Lead of Event Detection Team
National CyberSecurity Center

Source(s): Mastercard Advisors Analysis

HOW CAN MASTERCARD HELP IN FIGHTING CYBERCRIME?

WHAT ARE SOME CONCRETE SOLUTIONS?

- KEEPING SECURITY SYSTEMS UP TO DATE
- ENSURING THAT SUPPLIERS ARE ALSO PROTECTED
- ALWAYS STAY VIGILANT- ZERO TRUST POLICY
- BETTER UNDERSTANDING CYBERSECURITY RISK EXPOSURE

TO FIGHT THESE CHALLENGES AND PROTECT COMPANIES AND THE HOMO DIGITALIS SOCIETY, MASTERCARD OFFERS SOLUTIONS IN TWO MAIN PRODUCT CATEGORIES:

USER-FOCUSED

NUDETECT delivers real-time protection for online and mobile banking accounts, without disrupting the user's experience. This solution protects the end-to-end user journey throughout a digital banking session by assessing hundreds of device, location, passive biometric and behavioral signals against past user behavior types. By enabling even more frictionless real-time validation of users using passive biometric and behavioral data, NuDetect can help firms in adopting zero trust policies.

IT SYSTEMS-FOCUSED

Mastercard has multiple preventive solutions to support banks and merchants in estimating cyber risk and identifying areas of improvement by assessing their IT security systems.

RISKRECON is a cyber risk assessment product that is designed to assess, identify and mitigate cyber-based vulnerabilities within the digital ecosystem of a customer's enterprise and those of their third-party suppliers and vendors. Based on publicly available information, it provides a clear analysis of the customer's level of preparedness in terms of IT security, compares this to the sector and global competitors, and lists prioritized focus areas that the organization should consider for improvements.

CYBER QUANT assesses the current cyber-security risks based on a diagnostic survey, incorporating the current threat landscape into the risk assessment. By providing a quantified value of current risk and potential losses, this tool supports organizations in prioritizing investments in IT and security areas.

CYBER FRONT analyzes the organization's current IT systems based on their response to simulated cyber threats *(that do not affect the production system)*. This tool helps the organization be better prepared to fight fraudsters by identifying weak spots, continuously validating security, determining responses and improving defenses.

Source(s): Mastercard Advisors Analysis

PAYMENT FRAUD

CHAPTER 2

INTERNATIONAL

AND LOCAL TRENDS OF PAYMENT FRAUD

HUNGARY FACES
INCREASING
THREAT

PAYMENT FRAUD AFFECTS EVERY MAJOR PLAYER IN

THE PAYMENTS INFRASTRUCTURE

THE SIZE OF ANNUAL GLOBAL PAYMENT FRAUD IS EQUIVALENT TO ONE-FIFTH OF HUNGARY'S ANNUAL GDP. By developing an in-depth understanding of payment fraud trends, as well as prevention methods, organizations and private actors can equip themselves with the knowledge and tools necessary to stay resilient in a world that is increasingly threatened by payment fraud.

connect to address 192.168.1.1
username: *********
password: ***********
Access granted...
exited after 0.006146 seconds with return value
any key to continue . . .

$32B

In 2020, annual **GLOBAL LOSSES FROM PAYMENT FRAUD** climbed above **$32 BILLION** — a more than **TENFOLD INCREASE** over the past ten years.

+25%

It is estimated that **BY 2027,** global payment fraud losses will reach **$40 BILLION.** This corresponds to a **25% INCREASE** from the current value of payment fraud losses.

<1%

Despite the prevalence of payment fraud, **LESS THAN 1%** of funds suspected of payment fraud **ARE FROZEN OR CONFISCATED.** This indicates significant opportunities for players across the financial ecosystem to improve their fraud management methods, drive better business results, and create a more secure financial environment.

Source(s): MerchantSavvy; United Nations Office on Drugs and Crime

CARD TRANSACTIONS FRAUDS:
A GOOD EXAMPLE OF EFFICIENT CYBERWARFARE

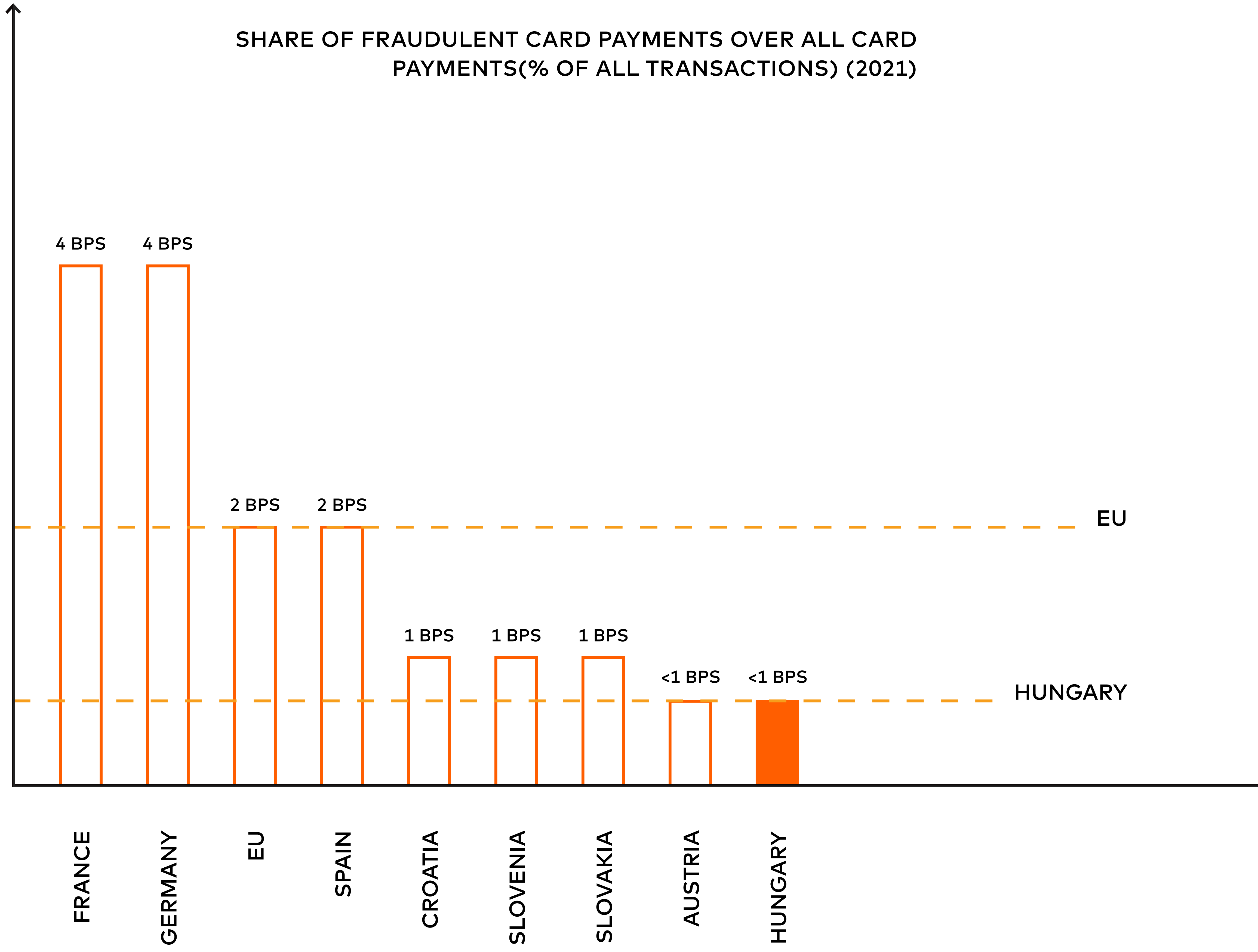
Despite the mammoth losses from fraud, the **SHARE OF FRAUDULENT CARD TRANSACTIONS IS RELATIVELY LOW** across Europe. In 2021, the fraud share for transactions within the **EU** around **2 BASIS POINTS**.

CARD FRAUD IS INFLUENCED
BY THREE MAIN FACTORS:

INCOME: Countries with higher median incomes offer more economic incentives for fraudsters due to the favorable risk-reward ratio.

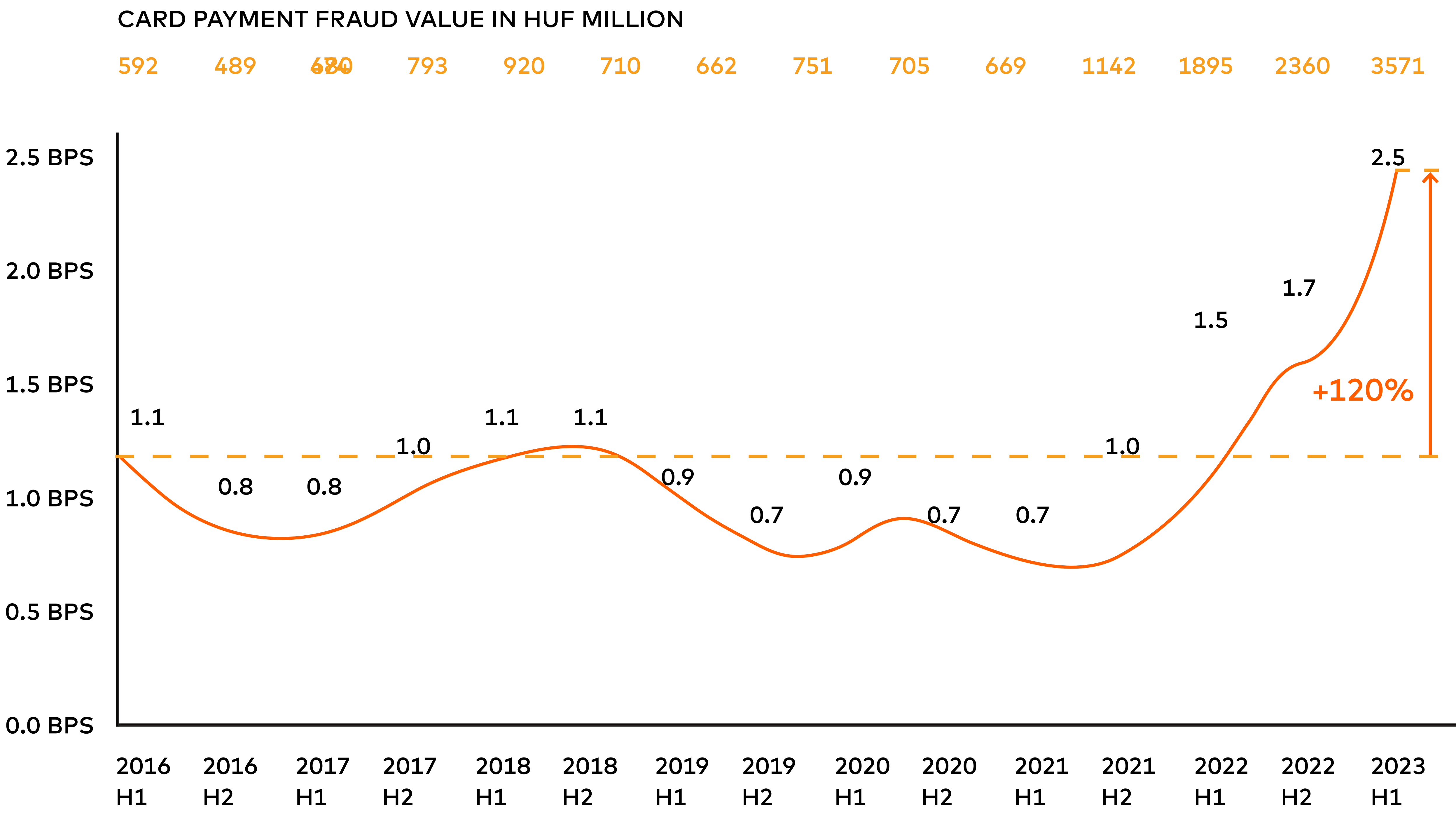
LANGUAGE: The more unique the language, the more difficult it is to carry out credible card fraud.

FINANCIAL EDUCATION: In more educated countries, fraud awareness is likely to be higher, with more sophisticated fraud prevention policies in place.



Source(s): European Banking Authority | (europa.eu)

CARD PAYMENT FRAUD IS SLIGHTLY INCREASING IN HUNGARY



Despite being on the top of the league, since the second half of 2017, the value had been steadily over 500 million HUF but started to increase sharply in 2021 and 2022. In the first half of 2022, the value has surpassed 3.5 billion HUF. Consequently, the fraud ratio has spiked as well, reaching 2.5 bps in the first half of 2023.

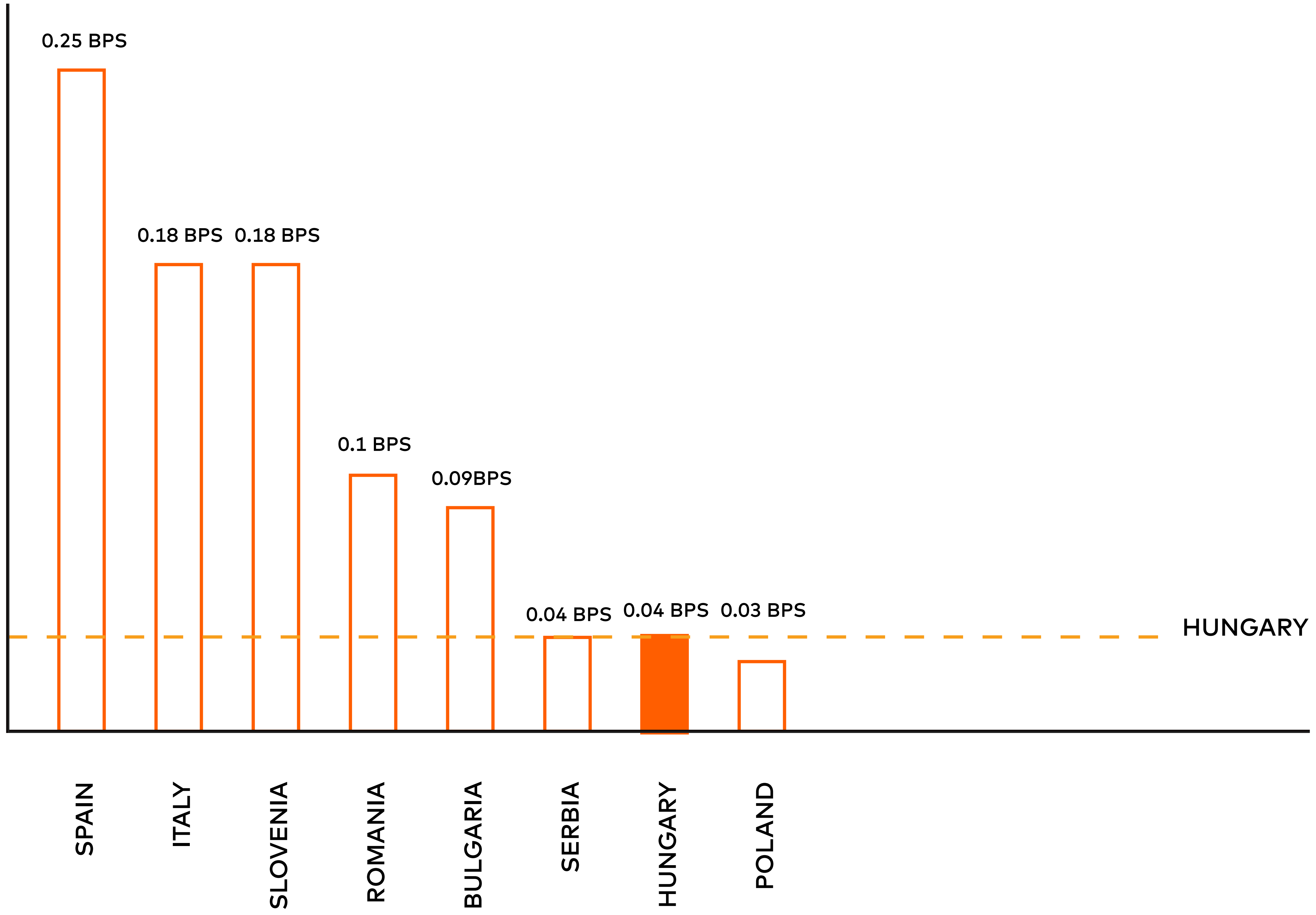
This sharp increase in card fraud over the last two years is largely due to the emergence of new types of fraud, targeting the Homo Digitalis community via **SOCIAL ENGINEERING** beyond stealing payment card credentials.

CARD PAYMENT FRAUD RATIO AND VALUE IN HUNGARY, FROM AN ISSUING PERSPECTIVE
(2016 H1 – 2023 H1) (BPS, HUF MILLIONS)

Source(s): Central Bank of Hungary (II.6; II.6.d; III.2a; III.2b)

CREDIT TRANSFER FRAUD

FRAUD SHARE FOR CREDIT TRANSFERS IN SELECTED COUNTRIES
(% OF TOTAL PAYMENT VALUE) (2020)



Source(s): European Banking Authority

CREDIT TRANSFER FRAUD REMAINS THE LOWEST across the European Economic Area – both in payment value and volume. In 2020, credit transfer fraud in the value of payments ranged from 0.03 to 0.25 basis points, with a median value of 0.1 basis point.

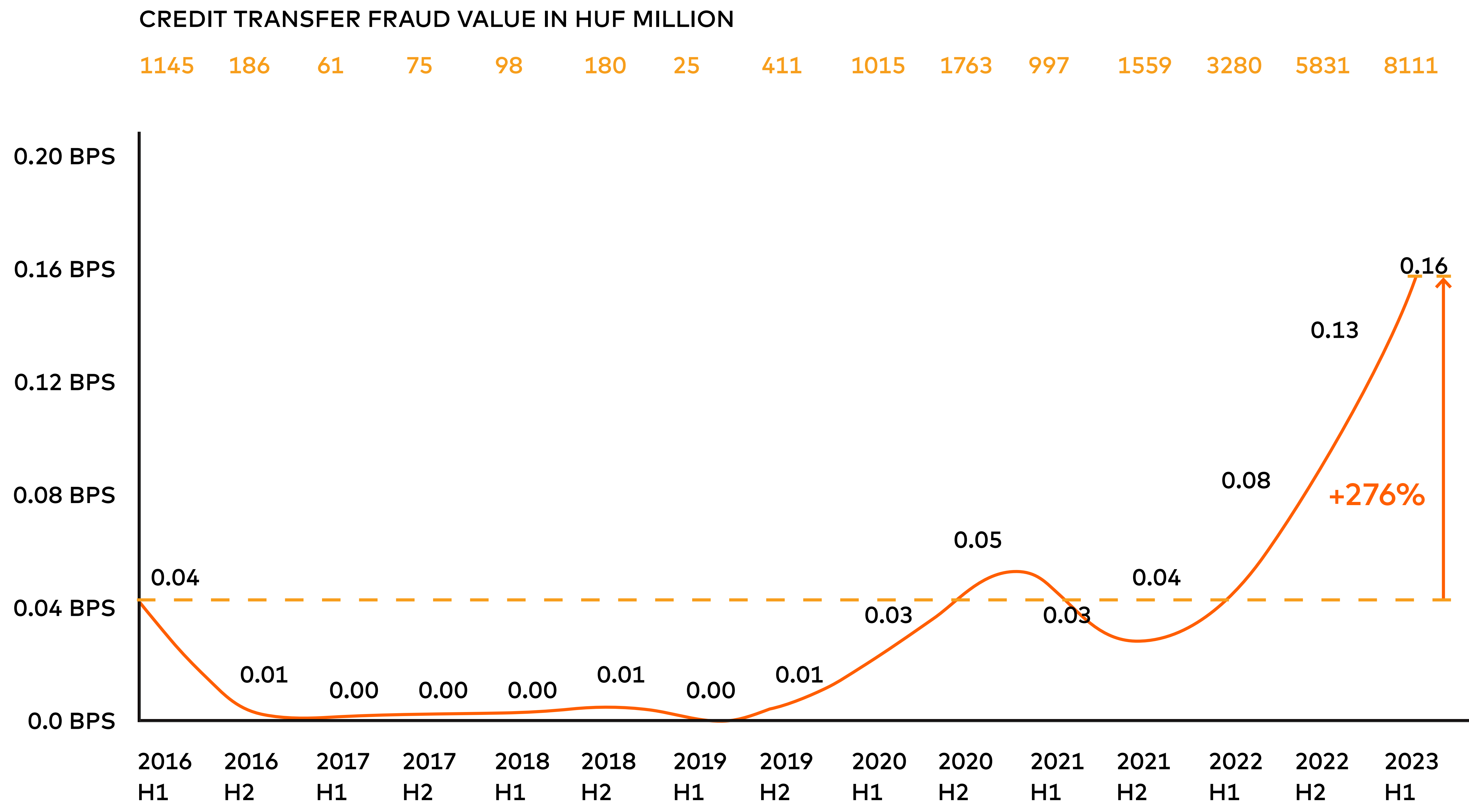
Of the reported fraudulent transactions, 94% were initiated electronically *(i.e., via any electronic platform)* and the rates were **THREE TIMES HIGHER** than for those initiated non-electronically.

Card fraud, however, demonstrates an opposite pattern. The card **PAYMENTS INITIATED NON-ELECTRONICALLY WERE FOUR TIMES MORE LIKELY TO BE AFFECTED BY FRAUD** than those initiated electronically.

For non-remote credit transfers – i.e., those not carried out via the internet or remote communication devices – **THE FRAUD RATE OF SCA-PROTECTED TRANSFERS WAS HALF THE RATE OF THOSE AUTHENTICATED WITHOUT SCA.** Within remote credit transfers, this trend was reversed.

The **FRAUD SHARE FOR SCA-AUTHENTICATED CREDIT TRANSFERS WAS ALMOST TEN TIMES LARGER THAN FOR THOSE NOT PROTECTED BY SCA,** potentially due to the higher risk factor of SCA payments. For instance, **SCA PAYMENTS** are more likely to involve forms of **SOCIAL ENGINEERING** on the part of fraudsters and thus carry a higher risk.

HUNGARY: SIGNIFICANT SPIKE IN CREDIT TRANSFER FRAUD RATIO AND VALUE OVER THE LAST TWO YEARS



From the second half of 2016 to 2019, the level of annual credit transfer fraud was below 1000 million HUF. **BY THE SECOND HALF OF 2020, HOWEVER, WITH THE GROWTH OF DIGITALIZATION, THIS NUMBER SPIKED TO OVER 1700 MILLION HUF.**

Reaching over **8 BILLION HUF AND 0.16 BPS** by the first half of 2023, credit transfer fraud in Hungary is still growing. When compared to card fraud, credit transfer fraud is lower in terms of basis points, but higher in terms of HUF value.

CREDIT TRANSFER FRAUD RATIO AND VALUE FOR ELECTRONIC PAYMENTS IN HUNGARY
(2016 H1 – 2023 H1) (BPS, HUF MILLIONS)

Source(s): Central Bank of Hungary (II.1; II.1c; III.8; III.9b)

TRANSACTIONS WITH SCA ARE ALSO HEAVILY AFFECTED BY FRAUD,

DUE TO SOCIAL ENGINEERING

Similarly to cards, users shifted towards using SCA, so did the **FRAUDSTERS.**[1]

Fraudulent SCA transactions grew from about 750 million HUF in H1 2020 to over 7.5 billion HUF in H1 2023 and climbed from 0.05 bps to 0.31 bps during the same time. Transactions without SCA remained on a fraud rate of around 0.02 bps for more than 2 years, reaching 0.03 bps for the first time in the second half of 2022.

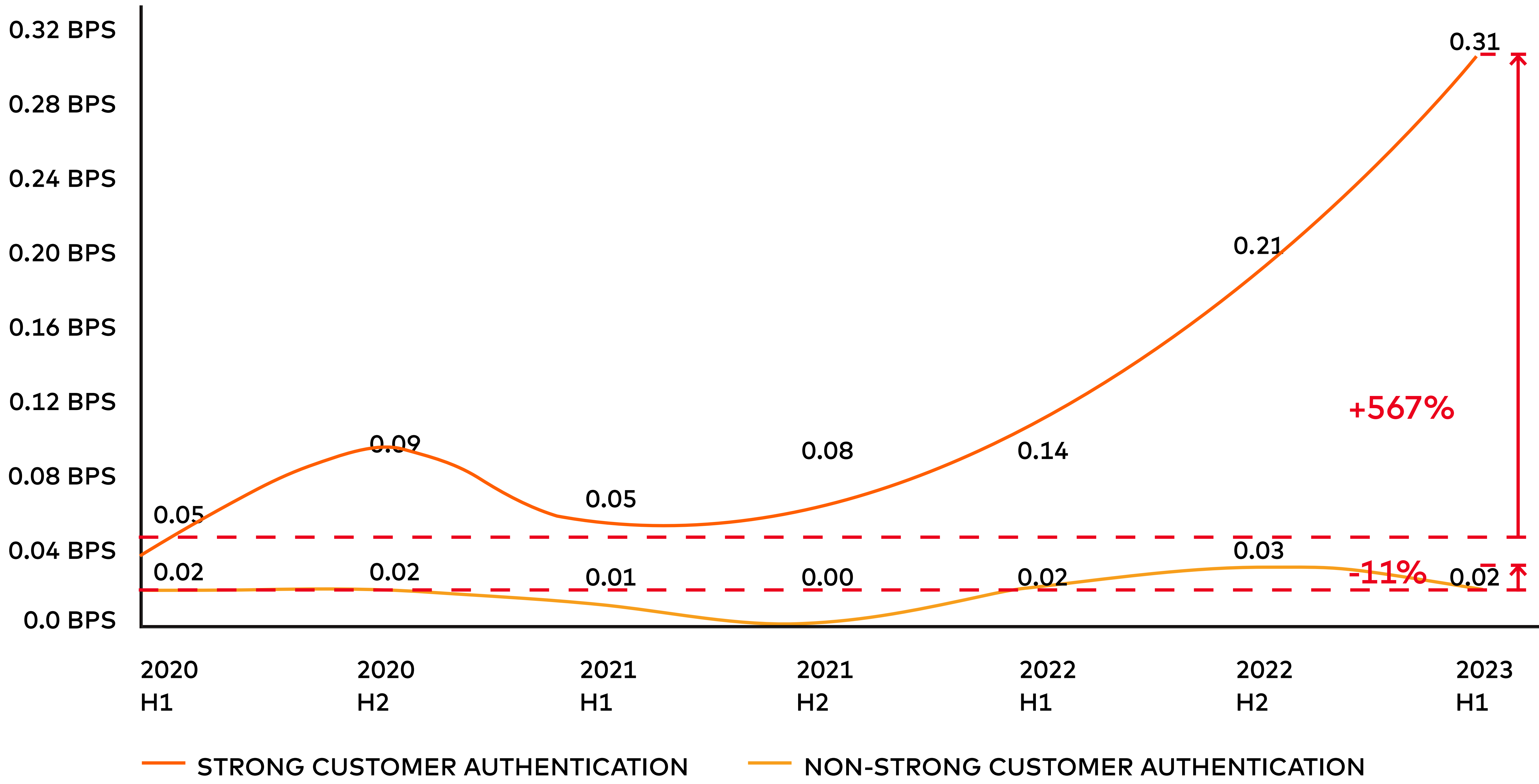
As in the EU, this trend clearly shows that while SCA provides increased security against unauthorized fraud, **CARDHOLDERS REMAIN SUSCEPTIBLE TO VARIOUS FORMS OF SOCIAL ENGINEERING** and fraudsters exploit the Homo Digitalis individuals' trust and trick them into authenticating fraudulent transactions.

CREDIT TRANSFER VALUE, SCA TRANSACTIONS IN HUF MILLION

748 1466 845 1494 2859 5137 7694

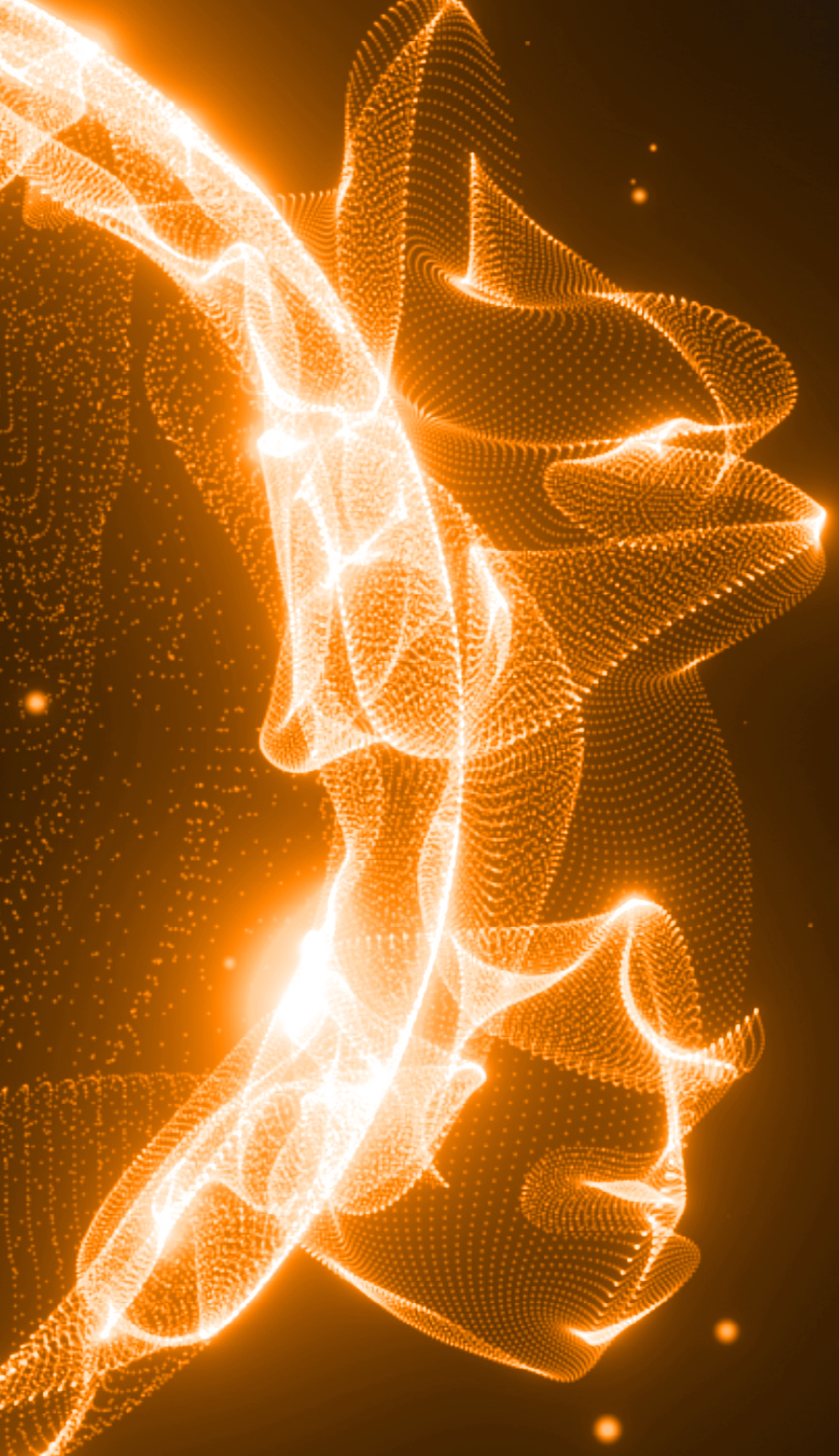
CREDIT TRANSFER VALUE, NON-SCA TRANSACTIONS IN HUF MILLION

268 297 152 65 421 694 417



CREDIT TRANSFER FRAUD RATIO AND VALUE FOR ELECTRONIC PAYMENTS WITH AND WITHOUT SCA IN HUNGARY
(2020 H1 – 2022 H1) (BPS, HUF MILLIONS)

Source(s): Central Bank of Hungary (II.1; II.1c; III.8; III.9b)



FRAUDSTERS ARE TURNING TO AUTHORIZED SCAMS TO EXPLOIT THE WEAKNESS OF HOMO DIGITALIS AS INFRASTRUCTURE IS MORE PROTECTED

As regulatory efforts and defensive mechanisms such as SCA took effect, fraudsters started using authorized scams that allow them to bypass these protective layers. This is further enabled by the growing level of digitization that allows low-cost and quick availability of information and infrastructure to facilitate these attacks. For example, fraudsters with minimal technical knowledge can easily rent call centers equipped with personnel via the dark web who will carry out the attacks. Very minimal specialized knowledge is required to set up scams on a large scale.

HUNGARIAN EXAMPLE: In 2021, police arrested a man living in the Dominican Republic who was the head of a real-estate fraud scheme in Hungary. He tricked victims into believing they were making legitimate real-estate purchases or rentals. He used multiple employees acting as assistants or solicitors to make the transactions seem realistic. While he was coordinating the scheme from South America, many of his employees were not aware they were engaged in illegal activity.

Source(s): Mastercard, Police.hu

ADDRESSING

THE CHALLENGES OF PAYMENT FRAUD

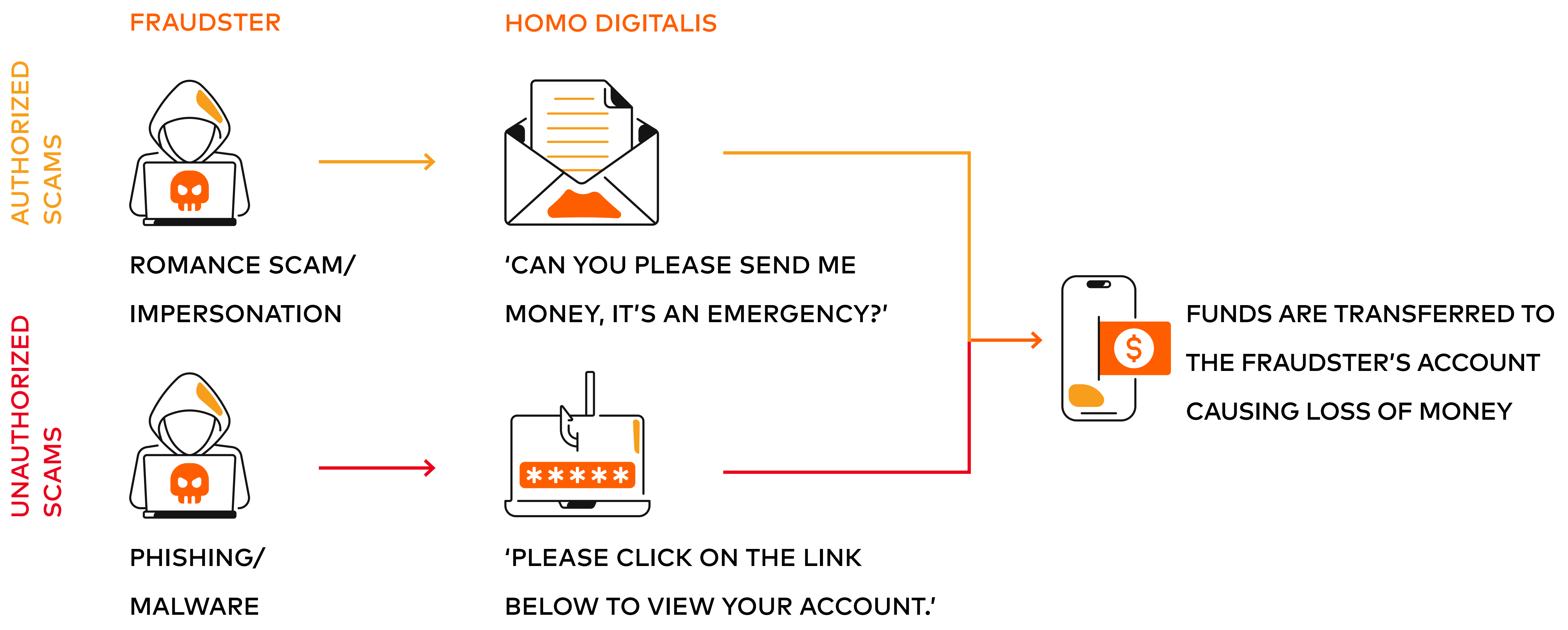
GOVERNMENTS, ORGANIZATIONS, AND CORPORATIONS STAND AT THE FOREFRONT OF CYBERATTACKS

PAYMENT FRAUD CAN BE CATEGORIZED INTO AUTHORIZED SCAMS AND UNAUTHORIZED ACCOUNT TAKEOVERS

BASED ON THE USERS' EXISTING PERMISSION

AUTHORIZED SCAMS:
Fraudsters use various types of social engineering to gain the trust of Homo Digitalis by contacting them via SMS, email or phone pretending to represent a trusted organization. Gaining the customer's trust allows fraudsters to manipulate them into initiating transactions or changing their payment data *(e.g., e-banking).*

UNAUTHORIZED ACCOUNT TAKEOVERS:
Fraudsters use sophisticated phishing and malware to intercept Homo Digitalis' authentication credentials to take over the account, allowing the fraudster to transfer funds to accounts under their control.



FRAUDSTER

HOMO DIGITALIS

AUTHORIZED SCAMS

ROMANCE SCAM/ IMPERSONATION

'CAN YOU PLEASE SEND ME MONEY, IT'S AN EMERGENCY?'

UNAUTHORIZED SCAMS

PHISHING/ MALWARE

'PLEASE CLICK ON THE LINK BELOW TO VIEW YOUR ACCOUNT.'

FUNDS ARE TRANSFERRED TO THE FRAUDSTER'S ACCOUNT CAUSING LOSS OF MONEY

Source(s): Mastercard, Police.hu

FIVE KEY TRENDS ARE SHAPING MODERN-DAY PAYMENT FRAUD

NEXT-GENERATION ACCOUNT TAKEOVERS

With the emergence of sophisticated forms of **SOCIAL ENGINEERING** and **DATA BREACHING,** customers' personal information is increasingly at risk.

RAMPANT IDENTITY THEFT

PROOF OF IDENTIFICATION and **ONLINE AUTHENTICATION PROCESSES** are becoming a fundamental need in the fight against identity theft.

INCREASED SOCIAL MEDIA USAGE

Social media is a common tool in **INVESTMENT AND ROMANCE SCAMS,** and money muling. With more time spent online, the susceptibility to social media scams is expected to rise in tandem.

SHIFTING MACROECONOMIC CONDITIONS

UNCERTAINTY IN THE BUSINESS ENVIRONMENT – such as COVID-19 and the Ukraine War – is incorporated into fraud tactics, leading to higher fraud vulnerability.

EMERGING PAYMENT TECHNOLOGIES

BUY NOW PAY LATER ACCOUNTS and cryptocurrency payments are often used in payment fraud due to the lower levels of regulatory oversight.

Source(s): Juniper Research

THE MOST PREVALENT PAYMENT FRAUD TYPES IN EUROPE: SOCIAL ENGINEERING, IDENTITY THEFT, CARD TESTING

TOP FRAUD ATTACK TYPES

PHISHING refers to attack types in which fraudsters try to steal funds by gaining access to victims' personal information such as credit card details.

WHALING *(also known as CEO fraud)* involves the impersonation of high-authority figures within an organization, with the impostors putting pressure on employees to provide their data.

PHARMING is another leading attack type, in which fraudsters aim to redirect online customers to a fake website.

IDENTITY THEFT is a potential consequence of social engineering. In this attack method, customers' details are stolen and used for fraud.

CARD TESTING involves fraudulent activity in which fraudsters determine the validity of stolen card details and then the availability of funds before conducting card fraud or reselling valid card details.

In the Americas, card testing is the most frequent attack method experienced by merchants. In North America – unlike other geographies – **FIRST-PARTY FRAUD** is also widespread. This attack type occurs without identity theft; it is the fraudsters themselves whose accounts are used for fraudulent activity, without involving victims or third parties.

Source(s): Juniper Research

FIVE CHALLENGES

ARE CRITICAL FOR BANKS, MERCHANTS, AND ACQUIRERS TO MANAGE FRAUD EFFECTIVELY

THE LACK OF A NETWORK-LEVEL OVERVIEW OF FRAUD

INADEQUATE AND SLOW REPORTING

THE PREVALENCE OF MONEY MULING

NOT KEEPING FRAUD MANAGEMENT SYSTEMS UP TO DATE

LOW FRAUD AWARENESS

Source(s): Mastercard Advisors Analysis

PAYMENT FRAUD CHALLENGES:

THE LACK

OF A NETWORK-LEVEL OVERVIEW OF FRAUD

HOW DOES IT HAPPEN?

- Most financial institutions lack the technology required for a **NETWORK-LEVEL OVERVIEW AND INTER-BANK COMMUNICATION:** as a result, the majority of banks only have access to their transactions and cannot follow fraudulent transactions outside their purview.
- Once a fraudulent transaction occurs, a top priority of fraudsters is to decrease traceability by distributing the acquired funds as quickly as possible into different accounts at different banks via multiple transactions.

WHAT YOU SHOULD DO?

- Consequently, for banks to efficiently identify and respond to fraud, they must have a system in place that facilitates communication among multiple financial institutions. Such a system allows all players affected by fraud to jointly leverage their fraud management systems, trace funds and reimburse victims.

HOW TO TAKE ACTION?

- Financial institutions must **1) IMPLEMENT SOLUTIONS THAT GIVE THEM ACCESS TO A NETWORK-LEVEL OVERVIEW** of fraud, instead of a single-party view; and **2) LEARN TO ENGAGE IN INTERPARTY** communication with other institutions to jointly leverage fraud management techniques.

"Banks need to work together to standardize their reporting and investigative processes to achieve a positive change. Today, money stolen via payment fraud can often not be traced anymore after a few hours due to quick shifts from account to account."

DANIEL WITTINGHOFF
Director
Cyber Business Development
Mastercard

Source(s): Mastercard Advisors Analysis

PAYMENT FRAUD CHALLENGES:

INADEQUATE

AND SLOW REPORTING

HOW DOES IT HAPPEN?

- There is no single, comprehensive reporting system that enables payment providers and financial institutions to track, report and analyze payment fraud patterns. In addition, most financial institutions have slow fraud-detection mechanisms that exacerbate the difficulty of reporting fraud.
- As a result, players in the financial ecosystem employ **DIFFERENT APPROACHES TO FRAUD REPORTING, WHICH MAKES IT MORE DIFFICULT TO DRAW CORRECT INSIGHTS FROM PREVIOUS INSTANCES** of fraud and mitigate future fraud.

WHAT YOU SHOULD DO?

- Players in the financial ecosystem need to **STREAMLINE THEIR REPORTING PRACTICES IN A UNIFIED MANNER.**

HOW TO TAKE ACTION?

- All stakeholders need to have **EFFICIENT AND CURRENT FRAUD MANAGEMENT SOLUTIONS** in place.
- They need to ensure that the solutions integrated into each player's internal system are based on the **SAME REPORTING PRINCIPLES.**

"Payment service providers need to implement real-time transaction monitoring systems that can evaluate the risk of each transaction based on the client's transactional and digital payment habits. This allows timely prevention even if the client was scammed previously but the payment has not happened yet. To ensure the acceptance of electronic payments, the enforcement of the *"Know your customer"* principle on a higher level is of outstanding importance. Similarly, the identification of those mule accounts that contribute to the rapid disappearance of the sums acquired during scams is also essential. In this case we can highlight the importance of the monitoring of transactional habits and client profiling once again."

MIKLÓS LUSPAY

Head of Financial Infrastructures Directorate

MNB

Source(s): Mastercard Advisors Analysis

PAYMENT FRAUD CHALLENGES:

NOT KEEPING FRAUD MANAGEMENT SYSTEMS UP TO DATE

HOW DOES IT HAPPEN?

- A rising number of players in the payments ecosystem find it challenging to stay up to date on new fraud prevention products as well as legislative or regulatory changes concerning payment fraud, enacting a significant barrier in fraud prevention

WHAT YOU SHOULD DO?

- Organizations – banks, merchants, and issuers alike – need to understand that **NO SINGLE FRAUD MANAGEMENT SYSTEM IS SOPHISTICATED ENOUGH** to withstand today's fraud tactics. Different solutions work for different types of fraud management.

HOW TO TAKE ACTION?

- **REACTIVE SYSTEMS** help organizations trace stolen funds ex post, thus allowing them to trace stolen funds, reimburse victims, and learn from past attacks.
- **PROACTIVE SYSTEMS,** on the other hand, complement an organization's fraud risk management processes by giving a priori insights into transactions and/or parties that are likely to be affected by fraud. For a comprehensive defense against fraud, a layered approach using various internal and external systems needs to be in place.

"No one fraud management system is good enough in itself. Organizations across the board must continue to implement various defensive layers into their fraud management solutions to efficiently manage fraud."

RICHARD LUFF
Vice President of Product Development, Mastercard

Source(s): Mastercard Advisors Analysis

PAYMENT FRAUD CHALLENGES:

LOW FRAUD AWARENESS

HOW DOES IT HAPPEN?

- Scams are becoming less and less linked directly to payment flows, meaning that they are not exploiting the deficiencies of the payment infrastructure anymore. As a result, their identification in the payment flow is an increasingly difficult task for all parties involved. Furthermore, customers cannot keep up with the rapid development of digitalization in terms of financial awareness and cybersecurity.

WHAT YOU SHOULD DO?

- By investing in educating stakeholders – both internal *(e.g., employees)* and external *(e.g., suppliers)* – on how to recognize and respond to fraud, organizations can **CREATE A SAFER WORK ENVIRONMENT AND ALSO PROTECT THEIR BOTTOM LINE** through lower fraud losses.

HOW TO TAKE ACTION?

- To improve fraud awareness, organizations must make it a priority to not only adhere to but also **STAY UP TO DATE ON PAYMENT FRAUD LAWS AND REGULATIONS.**
- Large-scale national campaigns also play a pivotal role in preventing and reducing payment fraud. In Hungary, in co-operation with the Hungarian Banking Association, the Central Bank of Hungary wishes to launch a nationwide consumer awareness campaign around cybersecurity and financial awareness.

"The criminals are trying to exploit this gap with methods that yield positive results with the use of promising offers or putting pressure on clients. Just to name a few usual stories we can mention fictitious investments, sweepstakes, emotional black mailings, or data theft via offering protection against pretended scams. We see the greatest challenge as the uniform education of consumers against these threats, as they are the first line of defense."

LAJOS BARTHA
Executive Director Financial Infrastructures
and Banking Operations, MNB

"The goal of the Cyber Security Educational Campaign is to ensure that consumers are constantly reminded of these messages via as many platforms as possible, to establish a habit that helps the consumers identify the scams using deception and psychological manipulation in time. The whole banking sector, card companies, governmental parties and investigative authorities are taking part in this collaboration."

LORÁNT VARGA
Head of Financial Infrastructure and
Payment Policy Department, MNB

Source(s): Mastercard Advisors Analysis

HOW MASTERCARD FIGHTS AGAINST PAYMENT FRAUD?

WHAT ARE SOME CONCRETE SOLUTIONS?

- ADOPT A NETWORK-LEVEL OVERVIEW OF FRAUD
- IMPLEMENT FAST AND EFFICIENT REPORTING PROCESSES
- MITIGATE MONEY MULING
- KEEP FRAUD MANAGEMENT SYSTEMS UP TO DATE
- IMPROVE FRAUD AWARENESS

MASTERCARD OFFERS SOLUTIONS IN TWO MAIN PRODUCT CATEGORIES:

REACTIVE (TRACE FINANCIAL CRIME)

Trace Financial Crime is the flagship product in the Mastercard portfolio of reactive fraud management solutions. The product helps banks and financial institutions detect fraudulent activity ex post, increasing the probability of recovering funds and protecting customers. Leveraging network-level insights instead of single-user data and paired with machine learning analytics, Trace Financial Crime improves users' fraud management tactics by extending the analysis of stolen funds to a higher level.

Following an instance of payment fraud, the product produces dispersion trees, showing the movement of funds between parties to enable traceability beyond the financial institutions' respective fraud systems. Furthermore, via its integrated track-and-trace algorithms, Trace Financial Crime notifies users of suspected mule accounts.

PREVENTIVE (PREVENT CONSUMER AND CORPORATE FRAUD)

The Prevent family of fraud management solutions allows financial institutions to fight payment fraud a priori as part of a pre-transaction screening process of account-to-account payments.

This product utilizes machine learning and bespoke analytics to learn from historic transaction patterns and ultimately determine the likelihood of a transaction involving fraud.

Following the analysis of a transaction, Prevent provides users with a score and the corresponding metadata to support the validation – or rejection – of a transaction. The product's operational impact is low, making it possible for financial institutions to integrate it with their systems seamlessly.

Source(s): Mastercard Advisors Analysis

APPENDIX

USE CASES: CYBERSECURITY SOLUTIONS

HOW CAN MASTERCARD HELP IN FIGHTING CYBERCRIME?

NUDETECT AT A GLANCE

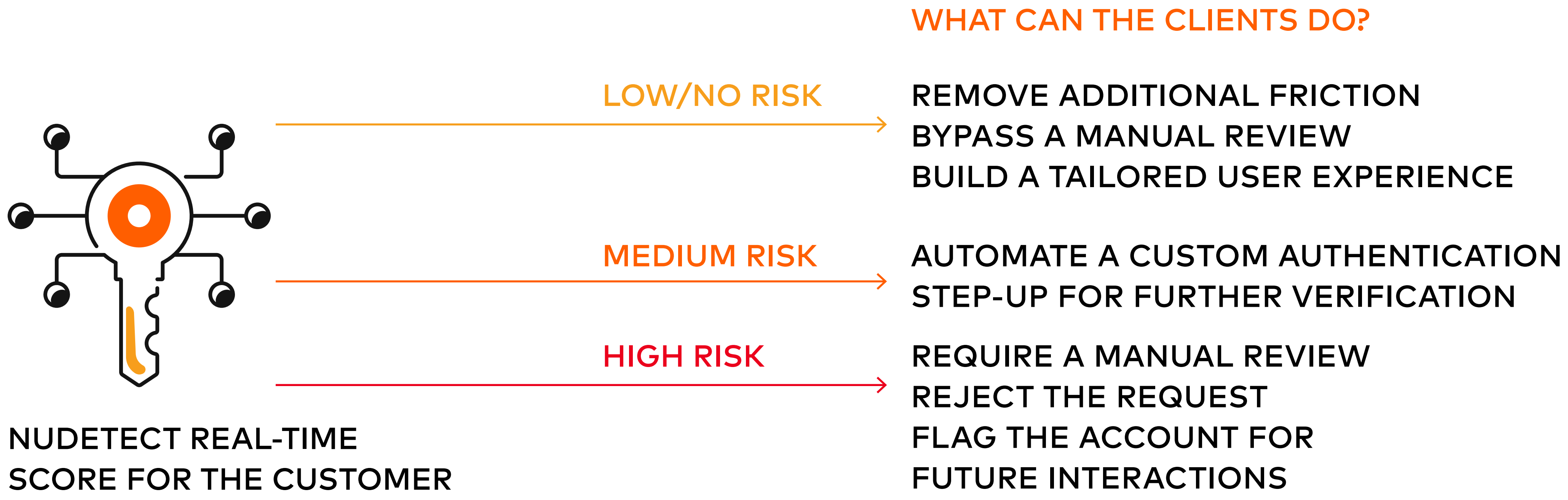
DESCRIPTION

NUDETECT delivers real-time protection for online and mobile banking accounts without disrupting the user experience. It analyzes the user's biometric and digital behavior to identify suspicious login attempts and registrations. A version is available for e-merchants and for the financial sector as well.

KEY BENEFITS

IMPROVE THE USER EXPERIENCE
DRIVE REVENUE
DECREASE FRAUD
REDUCE OPERATIONAL COSTS

HOW IT WORKS



WHAT CAN THE CLIENTS DO?

LOW/NO RISK → REMOVE ADDITIONAL FRICTION
BYPASS A MANUAL REVIEW
BUILD A TAILORED USER EXPERIENCE

MEDIUM RISK → AUTOMATE A CUSTOM AUTHENTICATION
STEP-UP FOR FURTHER VERIFICATION

HIGH RISK → REQUIRE A MANUAL REVIEW
REJECT THE REQUEST
FLAG THE ACCOUNT FOR FUTURE INTERACTIONS

NUDETECT REAL-TIME SCORE FOR THE CUSTOMER

Source(s): Mastercard

USE CASE

SITUATION

A well-established bank's authentication solution was adding too much friction to its customers' login experiences. With assets close to $200 billion, the institution evaluated NuDetect as a way to provide customers with a seamless, secure login.

CONTEXT AND APPROACH

The bank implemented the NuDetect behavioral biometrics solution to validate users at login. Following a two-week learning period, the software could recognize the users based on their behaviors. Evaluating data from a subpopulation of the bank's traffic that was processed through the behavioral biometrics solution, the results showed great accuracy.

RESULTS

- **NEARLY 2.5X MORE RECOGNIZED USERS** at login compared with the use of traditional device and network-layer tools
- **91% OF USERS RECOGNIZED** after 14-day training period
- **0.01%** false positive rate
- **13 MILLION** total events analyzed

HOW CAN MASTERCARD HELP IN FIGHTING CYBERCRIME?

RISKRECON AT A GLANCE

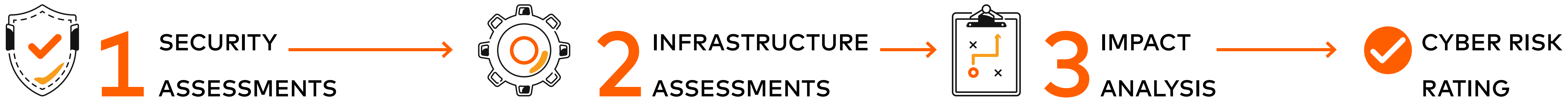
DESCRIPTION

RISKRECON is a cyber risk assessment product that is designed to assess, identify and mitigate cyber-based vulnerabilities within the digital ecosystem of a customer's enterprise and those of their third-party suppliers and vendors by analyzing the URL code.

KEY BENEFITS

REDUCE FINANCIAL LOSSES from third-party cyber risk
GAIN GREATER CONTROL and flexibility managing third-party cyber risk
SAVE TIME and resources managing third-party cyber risk
OBTAIN MORE RELIABLE, ACCURATE ASSESSMENTs of third-party cyber risk

HOW IT WORKS



1 SECURITY ASSESSMENTS

Evaluate security measures in place to combat risks like malware and ransomware

- Email security
- Breach events
- Network filtering
- DNS security
- System reputation

2 INFRASTRUCTURE ASSESSMENTS

Assess software and hardware system risks

- Web encryption
- Application security
- Software patching
- System hosting

3 IMPACT ANALYSIS

Analyze the impact of each issue uncovered based on its criticality as well as sensitivity of the system where it was identified

CYBER RISK RATING

Source(s): Mastercard

USE CASE

SITUATION

A large global financial institution had significant resource constraints in assessing the cyber risk posed by third-party service providers. Every full-time employee within the risk management team was only able to assess a few dozen third-party service providers each year due to the complexity of the process.

CONTEXT AND APPROACH

RiskRecon enabled the financial institution to automate the cyber risk assessments of their third-party service providers. With only minimal manual intervention required, the product helped reduce the strain on the financial institution's resources.

RESULTS

10,000+ THIRD-PARTY SERVICE PROVIDERS MONITORED WITH MINIMAL MANUAL INTERVENTION

After the assessment, the financial institution:

- Assigned risk categorizations and priorities to different third-party providers
- Took actions after assessing accurate data
- Started a process to track third-party service provider risk when new cyber threats surface

HOW CAN MASTERCARD HELP IN FIGHTING CYBERCRIME?

CYBER QUANT AT A GLANCE

DESCRIPTION

CYBER QUANT assesses the current cybersecurity risks based on a diagnostic survey, incorporating the current threat landscape into the risk assessment. By quantifying the value of current risk and potential losses, Cyber Quant supports organizations in prioritizing investments in IT and security areas.

KEY BENEFITS

IDENTIFY CRITICAL SECURITY GAPS by assessing the maturity of over 50 cybersecurity capabilities and the importance of each

QUANTIFY CYBERSECURITY RISKS specific to the organization and calculate the potential financial impact of a breach

PRIORITIZE NEXT STEPS to improve security posture and reduce risk by conducting simulations to pinpoint actions with the greatest ROI

HOW IT WORKS

Cyber Quant takes an inside-out approach to identify and quantify the cybersecurity risk of businesses and runs simulations to prioritize risk mitigation actions with the greatest ROI.

Source(s): Mastercard

USE CASE

SITUATION

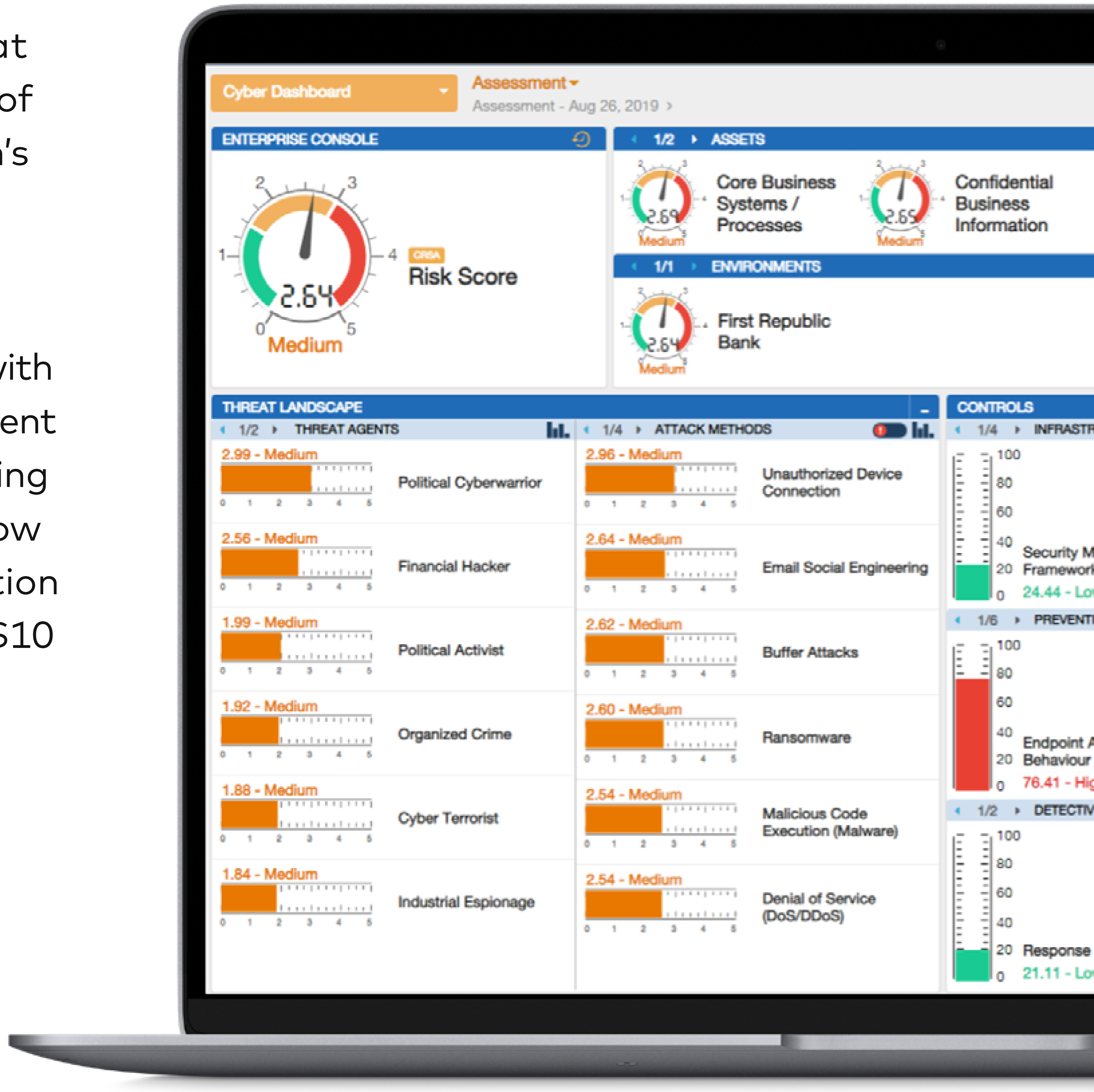
The Chief Information Security Officer at a national bank was facing the challenge of how to focus and prioritize the organization's limited resources for maximum impact.

CONTEXT AND APPROACH

The bank conducted a Cyber Quant study with Mastercard, which analyzed the bank's current cyber posture and recommended prioritizing three controls – a strategy that would allow the bank to achieve a $155 million reduction in potential financial loss with less than $10 million in cyber-security investments.

RESULTS

As a result of the engagement, the bank maximized the effectiveness of their limited resources and decreased financial risk by $155 million.



HOW CAN MASTERCARD HELP IN FIGHTING

CYBERCRIME?

CYBER FRONT AT A GLANCE

DESCRIPTION

CYBER FRONT analyzes the organization's current systems using simulated cyberthreats *(that do not affect the production system)* to continuously validate security, determine responses and improve defenses.

KEY BENEFITS

VALIDATE that security infrastructure, configuration settings and prevention technologies are operating as intended

CONTINUOUSLY test existing security infrastructure, without the need to wait for vulnerability scanning windows

UNDERSTAND THE PROBABILITY OF A THREAT by identifying threats and attack vectors

ENSURE SECURITY OPS STAFF AND INCIDENT RESPONDERS CAN DETECT ATTACKS and respond accordingly during cyber response exercises

WHAT MAKES CYBER FRONT STAND OUT

- Mastercard team collaborates with the customer to set up the platform for enabling ongoing simulation tests based on 9000+ unique threats and 500+ unique scenarios resulting in better identification of threats to address
- Threats and scenarios are updated daily
- The tested incident and threat types, results and recommended solutions are displayed on a central dashboard

HOW IT WORKS

1 Mastercard consultants analyze the current network structure and provide guidance for the optimal Cyber Front deployment architecture.

2 The system admin deploys simulation agents and initiates assessments, with results in minutes and detailed analysis in just hours.

3 Cyber Front provides recommendations specific to the organization's security technology vendors from Cyber Front's prevention database of widely-used technologies.

4 Mastercard provides coaching to prioritize and implement recommendations, including integration with Cyber Quant, for prioritized risk remediation.

5 The system admin implements the recommendations while Mastercard consultants prepare playbooks for response scenarios based on the identified prioritized attacks.

6 Continuous simulations measure security posture improvements and monitor for new threats.

Source(s): Mastercard

USE CASES: PAYMENT FRAUD SOLUTIONS

HOW CAN MASTERCARD HELP IN FIGHTING

PAYMENT FRAUD?

TRACE FINANCIAL CRIME AT A GLANCE

DESCRIPTION

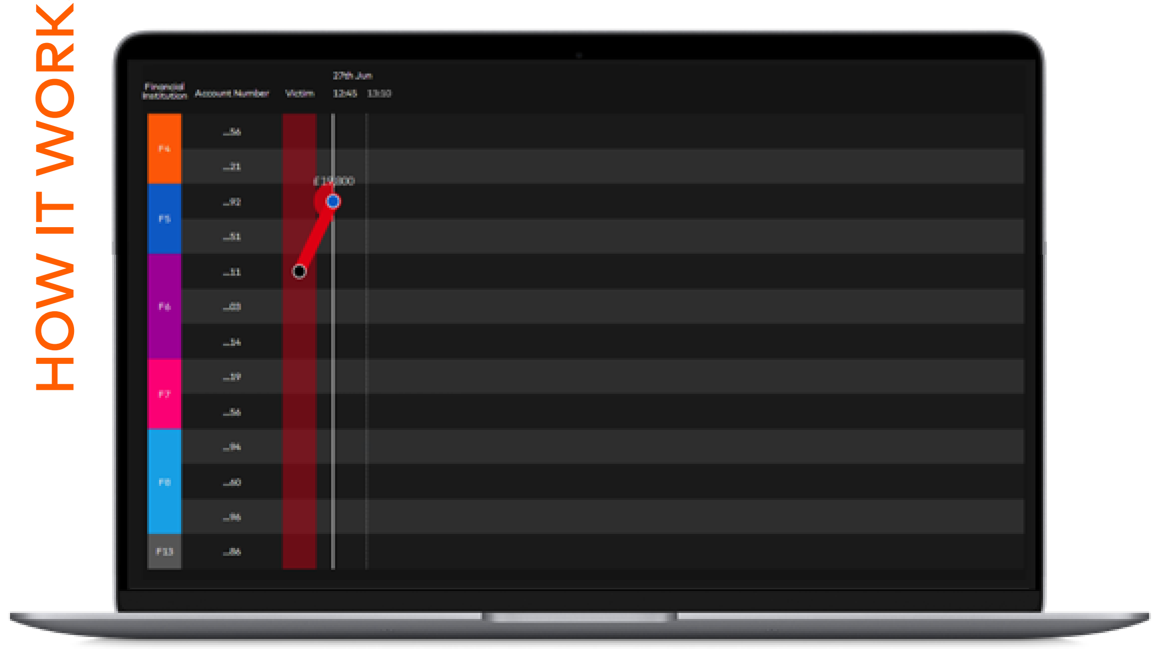
Trace Financial Crime helps banks and financial institutions detect fraudulent activity ex post, and thus increase the probability of recovering funds and protecting customers. Leveraging network-level insights instead of single-user data and paired with machine learning analytics, Trace Financial Crime improves users' fraud management tactics by extending the analysis of stolen funds to a higher level.

KEY BENEFITS

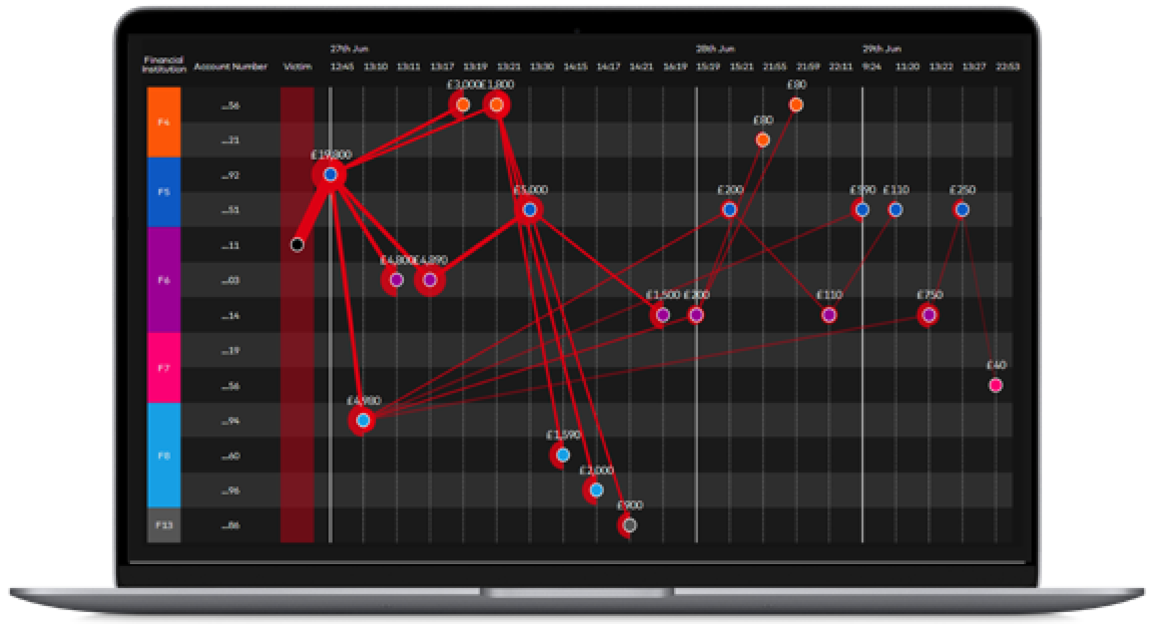
IDENTIFY suspect money laundering accounts
AVOID fines from regulatory bodies
CREATE efficiencies and cost savings
PROTECT the company's reputation and customers' assets

HOW IT WORKS

WHILE BANKS ONLY SEE THEIR OWN ACCOUNT



TRACE ALLOWS A NETWORK LEVEL OVERVIEW



USE CASE

SITUATION

A bank was notified by a customer that they were a victim of fraud. The details of the fraudulent transaction were uncovered using Trace Financial Crime.

CONTEXT AND APPROACH

The account was a fourth-generation mule account within a complex network. The account activity was typical of a mule: receiving large volumes of funds and rapidly paying them out. The majority of funds were being sent to another account within the same bank, which was found to be receiving large volumes of funds and distributing them further.

RESULTS

As investigations progressed, a fraud ring of over 70 active accounts was uncovered and shut down.

Source(s): Mastercard

HOW CAN MASTERCARD HELP IN FIGHTING

PAYMENT FRAUD?

PREVENT CONSUMER AND CORPORATE FRAUD AT A GLANCE

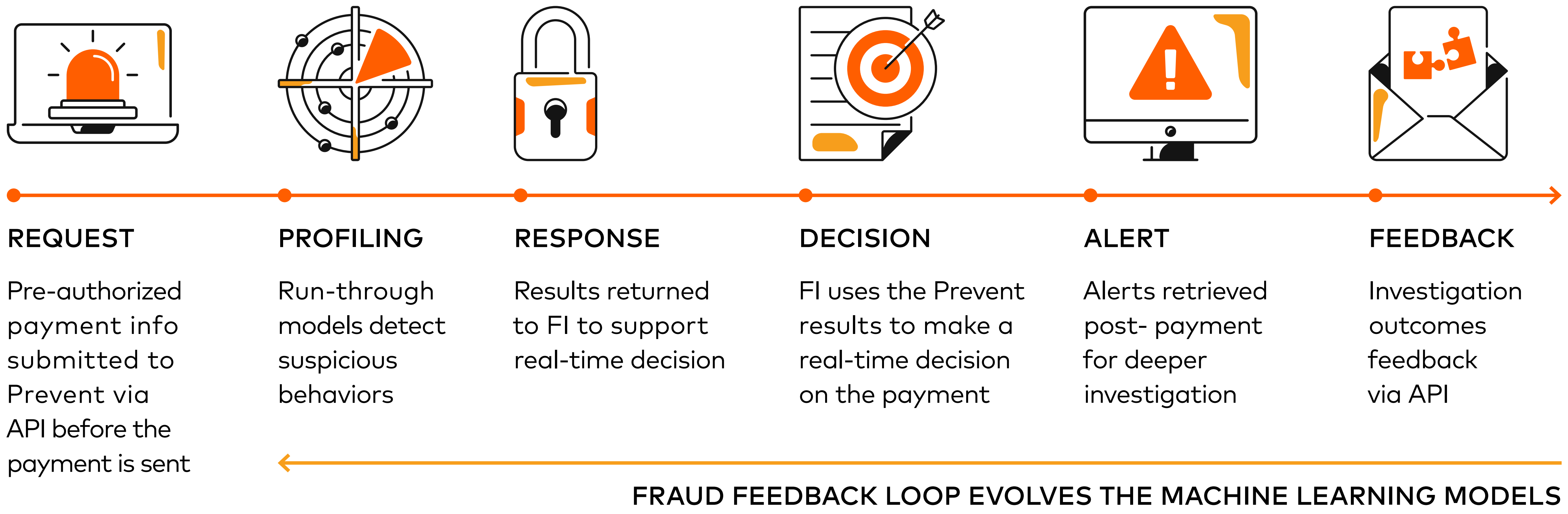
DESCRIPTION

This preventive fraud management solution enables financial institutions to fight payment fraud a priori as part of a pre-transaction screening process of account-to-account payments.

KEY BENEFITS

PREVENT customer losses
DIFFERENTIATE and protect the institution's reputation
CREATE EFFICIENCIES and generate cost savings

HOW IT WORKS



REQUEST
Pre-authorized payment info submitted to Prevent via API before the payment is sent

PROFILING
Run-through models detect suspicious behaviors

RESPONSE
Results returned to FI to support real-time decision

DECISION
FI uses the Prevent results to make a real-time decision on the payment

ALERT
Alerts retrieved post- payment for deeper investigation

FEEDBACK
Investigation outcomes feedback via API

FRAUD FEEDBACK LOOP EVOLVES THE MACHINE LEARNING MODELS

USE CASE

SITUATION

A major financial institution entered into a partnership with Mastercard to better understand the impact of scams on consumer account-based payments.

CONTEXT AND APPROACH

As a result of the partnership, a solution was designed and built to address the issue of scams on consumer account-based payments. The positive results led the financial institution to characterize Prevent Retail Payment Fraud as a fundamental game-changer, unlike anything they had encountered.

RESULTS

+50% average incremental volume detection rate vs. previously missed frauds
76% average total value detection rate across all frauds
21:1 lower average false positive ratio than existing solutions

Source(s): Mastercard

THANK YOU!

CONTACT US:

TAMÁS RACSKÓ
DIRECTOR
PRODUCTS & SOLUTIONS
TAMAS.RACSKO@MASTERCARD.COM

MÁTÉ NEMES
PRODUCT DEVELOPMENT MANAGER
MATE.NEMES@MASTERCARD.COM

ROBERT GEISZT
CONSULTANT
ROBERT.GEISZT@MASTERCARD.COM

DANIEL WITTINGHOFF
BUSINESS DEVELOPMENT DIRECTOR
DANIEL.WITTINGHOFF@MASTERCARD.COM

SOURCES

1. Digital-operational-resilience-act.com: The official website of the DORA initiative https://www.digital-operational-resilience-act.com/
2. European Central Bank: Seventh report on card fraud by the European Central Bank (October 2021) https://www.ecb.europa.eu/pub/pdf/cardfraud/ecb.cardfraudreport202110~cac4c418e8.en.pdf
3. European Banking authority: Discussion Paper on EBA's preliminary observations on selected payment fraud data under PSD2, as reported by the industry (January 2022) https://bit.ly/3TFo5ec
4. European Commission SMEs and Cybercrime 2022 Survey, Ipsos: Flash Eurobarometer - SMEs and Cybercrime (December 2021) https://europa.eu/eurobarometer/surveys/detail/2280
5. Central Bank of Hungary: Fizetési forgalom - II.1, II.1c, II.6, II.6d - (March 2023) https://statisztika.mnb.hu/idosor-1020
6. Central Bank of Hungary: Pénzforgalmi visszaélések - III.2a, III.2b, III.8, III.9b - (March 2023) https://statisztika.mnb.hu/idosor-1024
7. Juniper research: Online Payment Fraud: Market Forcast, Emerging threats & Segment analysis 2022-2027 (July 2022) https://www.juniperresearch.com/researchstore/fintech-payments/online-payment-fraud-research-report
8. Mastercard Cyber Quant platform: Proprietary platform of Mastercard - Data gathered from 14 data sources including: Mastercard threat intelligence, cybersecurity event reports, dark web websites, hacker forums, RSS feeds
9. Merchant savvy: Global Payment Fraud Statistics, Trends & Forecasts (October 2020) https://www.merchantsavvy.co.uk/payment-fraud-statistics/
10. Police.hu: Dominikán vágták le a bűnszervezet csápjait (October 2021) https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/dominikan-vagtak-le-a-bunszervezet-csapjait
11. Ponemon institute: Data Risk in the Third-Party Ecosystem (October 2022) https://www.riskrecon.com/ponemon-report-data-risk-in-the-third-party-ecosystem-study
12. Prolifics testing: The Most Common Responses To Cyber-Crime In European Countries https://www.prolifics-testing.com/the-most-common-responses-to-cyber-crime-in-european-countries
13. Reuters: Hungary hit by large cyber attack from Asia -Magyar Telekom (September 2020) https://www.reuters.com/article/hungary-cyber-idUKL5N2GN03J
14. Statista 2020: Cyber risk in selected Central and Eastern European (CEE) countries in 2020 (February 2021) https://www.statista.com/statistics/1202279/cee-vulnerability-to-cybercrime/
15. United Nations Office on Drugs and Crime: Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes (2011) https://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf
16. EUR-Lex - 32022R2554 - EN - EUR-Lex (europa.eu)
17. European Banking Authority | (europa.eu)