Information session on Fraud & AI

21 November 2024

WORLDLINE

febelfin

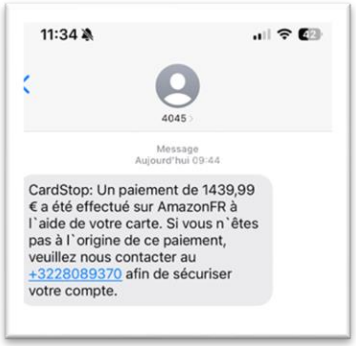
Fraud in Belgium

Top 3 trends : phishing

Phishing is a scam where fraudsters pretend to be a trusted organization in an attempt to retrieve personal banking codes.

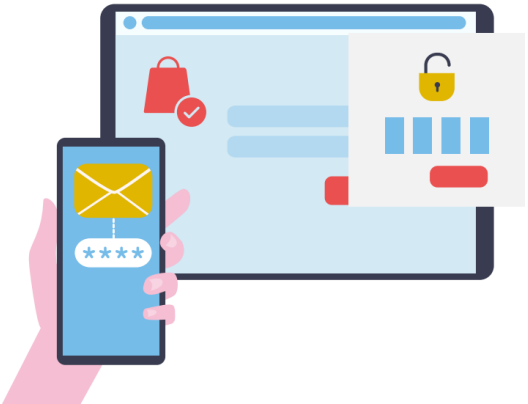
They send a **message** (email, SMS) containing a link to a fake website or malicious software.

Phishing can also be done over the **phone**.



Tips

Reliable organizations will **never ask** for your banking information via a link in a text message, email, or over a phone call.



New forms of online fraud are emerging

The types of online fraud in which victims make transfers due to manipulation by cybercriminals continue to rise.

These practices are generally little known or even completely unknown by Belgians. On average, slightly **less than one in five** Belgians understand what these types of fraud entail, **33%** have heard about them, but **nearly half** of the population is completely in the dark.

Top 3 trends : investment fraud

Fraudsters offer investments **with very high returns.**

Investment fraud usually starts on **social media**, where numerous ads promise extraordinary returns to those willing to take a chance. These ads often lead to websites promoting attracting services such as trading platforms, apps (using artificial intelligence), or training programs, all claiming to help you get rich quickly and without risk.

Victims invest their money **but lose all of it.**

Tips (FSMA)

- Know who you are dealing with
- Be wary if you receive an unsolicited phone call
- Ask for information about what you are being offered
- Be sceptical if the person or company contacting you is based abroad or if you are asked to transfer money to a foreign bank account
- Never respond to an investment or credit offer made by telephone or email
- Never take a quick investment decision
- Never pay fees that are not clearly explained, requested by persons you don’t know
- Never accept an offer that seems to be too good to be true
- …

Top 3 trends : CEO fraud

Fraudsters pretend to be the CEO of a company (or a trusted internal or external person) to manipulate an internal employee into making an "urgent and confidential" payment.

The fraudsters start by gathering information.

After that, they contact one or more employees responsible for payments (e.g. in the accounting department) and impersonate the CEO.

CNN

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

A finance worker at a multinational firm was tricked into paying out $25 million to fraudsters using deepfake technology to pose as the...

4 févr. 2024

Tips

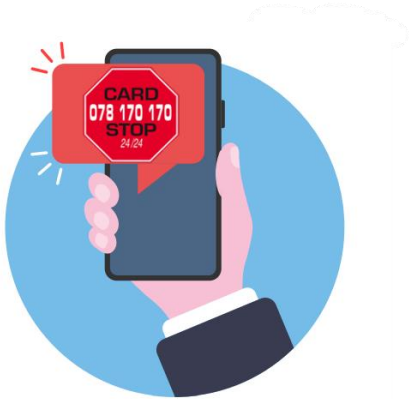
- Check the sender's email address.
- Be vigilant for "confidential" orders to urgently transfer large sums of money.
- If you receive such an urgent request, always call the requester using a phone number you know.
- Never leave a dual signature in the hands of a single person (cards and PIN codes).
- Ensure there are sufficient control measures in place.

Did you fall into the trap?

—Immediately block your bank cards if you have shared your card information by calling Card Stop.

—**Contact your bank as soon as possible**. You can find the contact details for banks on the Card Stop website. Banks have specific fraud services available 24/7.

—File a complaint with the police.



Some figures

In 2023, fraudsters were able to steal more than **€ 40 M** by phishing

8% of Belgians report to have been a victim of phishing

In 2023, Belgian consumers reported having more than **€15,482,000** stolen by fraudulent trading platforms (FSMA)

40% have never heard of investment fraud

Victims of fraud include youngsters as well

—Young people are also victims of fraud and may fall into traps more easily due to a lack of awareness.

- **27%** of those aged 16 to 30 do not know what phishing is (4% for the 31-79).
- **10%** say they have already been victims of phishing (7% for the 31-79).
- **7%** of young people would give their bank code without hesitation if the “bank” asked them to (1% for the 31-79).
- **1 out of 4** young people follow the investment advice of a celebrity or influencer.

Money mules: young Belgians particularly targeted by recruiters

- A recent survey conducted by Febelfin highlights a concerning trend among young Belgians, underscoring the increasing vulnerability to becoming money mules.
- The 2024 study results reveal that 6 in 10 young people who are offered to act as a money mule would lend their bank card and PIN and make their bank account available in exchange for a remuneration.
- Criminals need intermediary bank accounts to deposit money obtained illegally through online scams, quickly transfer the money, or withdraw it in cash immediately. With money mules, criminal organisations can carry out significant fraud while reducing their exposure to risks (be traced and arrested).

Banks are making significant efforts to prevent fraud

- Two-step authentication: The customer identifies themselves using two elements (card/phone & PIN code/fingerprint/facial recognition) to make electronic payments.
- Intensive transaction monitoring: **75%** of all fraudulent transfers due to phishing are detected or recovered.
- Close cooperation with telecom companies (for smishing and spoofing), the public prosecutor's office, the justice system, the police, and others.
- Mule stop: It allows the victim's bank to request the money mule's bank to block the fraudulently transferred amount.
- Coming soon
  - IBAN-name check: This will indicate during the initiation of a credit transfer whether the account number belongs to the payee.

Awareness raising

— March 2024

Febelfin campaign in collaboration with well-known influencers, targeting **investment fraud**. From Dubai, the influencers urged their followers to follow their financial advice and join their private Telegram group to "get rich quickly." By the end of the story, the followers discovered that it was all a huge scam. This emphasized the need to stay vigilant against investment fraud committed by fake "finfluencers" on social media. Through this campaign, Febelfin reached a large number of young people.

Awareness raising

—September 2024

Two-step verification or Two Factor Authentication (2FA) is a simple solution to better protect your accounts.

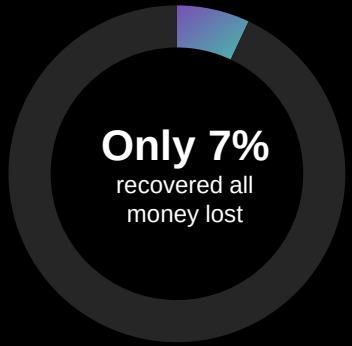
Usually, you only use one element (e.g., a password or PIN) to prove your identity. BUT it is better to use two or more factors: we call this two- or multi-step verification (2FA or MFA). For example, you can use a password and also have a code sent to your mobile phone, or you can use your fingerprint along with an authentication app to gain access.
With two-step verification, you can keep unwanted individuals at a distance, even if they know your password.
80% of online fraud can be avoided!

—November 2024 : Febelfins campaign to warn about various forms of online fraud, such as phishing, investment fraud, and friendship/dating fraud.

AI & fraud

Fraud Trends

State of Scams Report 2023



GASA
Global Anti-Scam Alliance

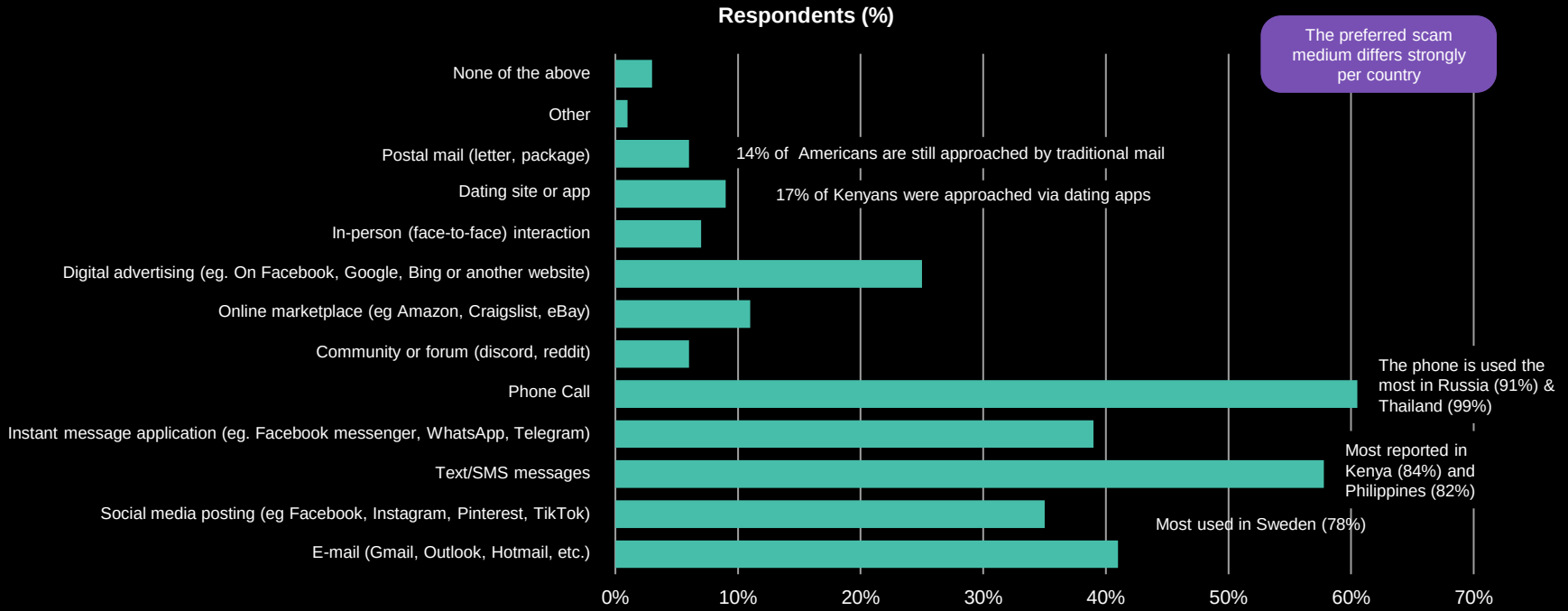
49,459
participants in the report

43
countries

>50%
participants with University
or Post Graduate

WORLDLINE

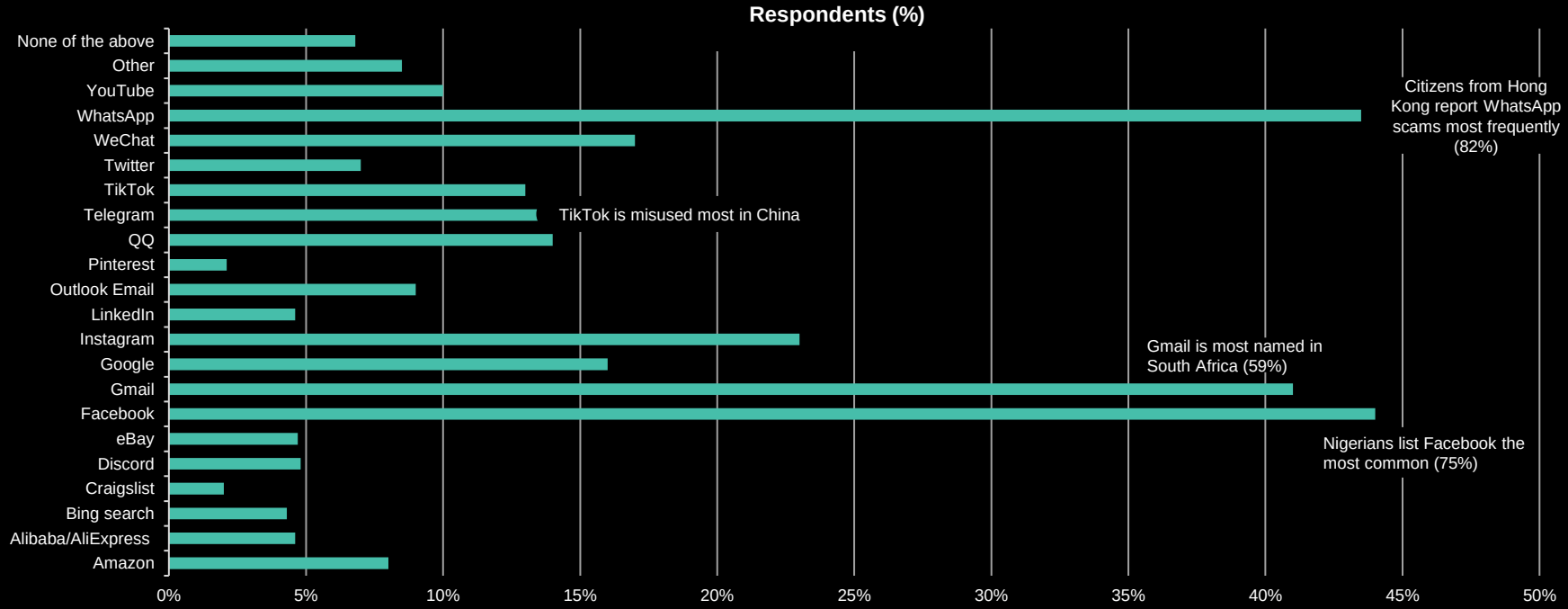
Phone (61%) and Text/SMS messages (58%) are the most common scam media



Followed by E-mail (40%) and instant messaging apps. Traditional mail and face-to-face scams are the least common methods of scamming people (each 6%).

Q5. Through which communication channel(s) did scammers mostly try to approach you in the last 12 months? Choose up to 3.

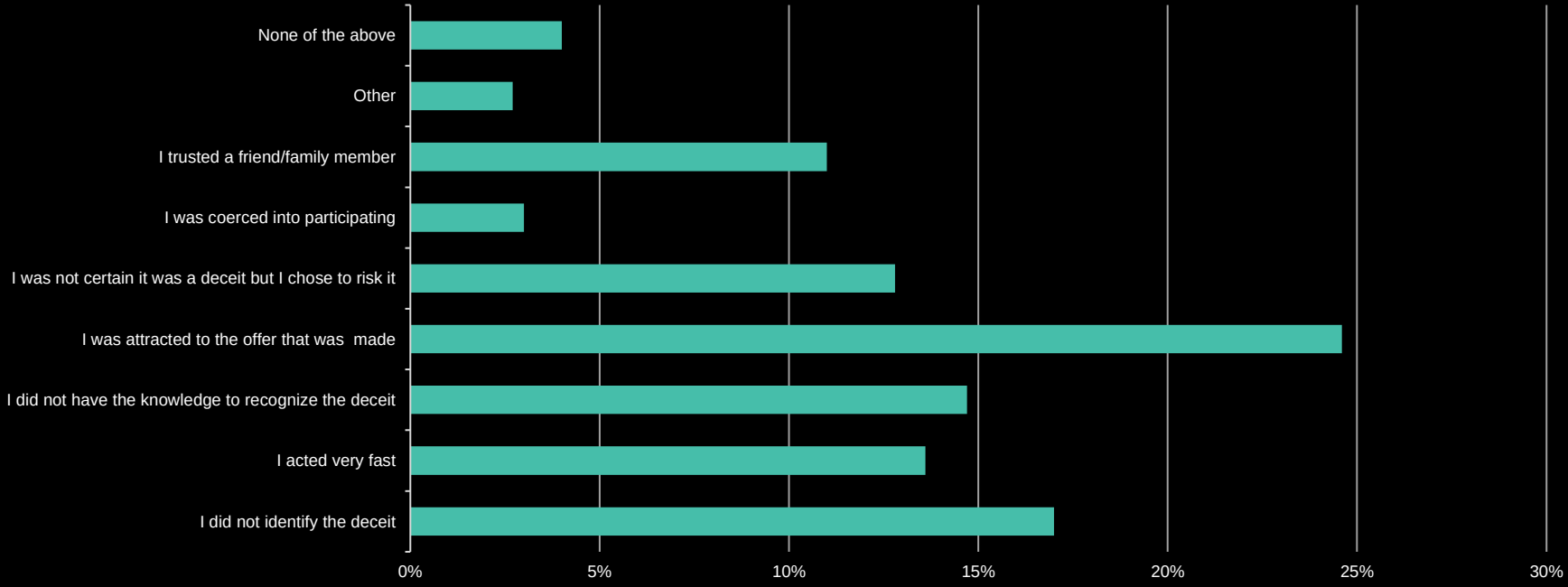
Facebook and Whatsapp (both named 44%) are the platforms most used by scammers



The third place is taken by Gmail (41%). Local players are also named such as Yahoo!, Shopee, Line & Mercari.

Q6. Via which platform9s) did scammers mostly try to contact you in the last 12 months? Choose up to 3.

The main reason people are scammed is being confronted by an attractive offer



However, not identifying the deceit or lacking the knowledge to recognize the scam take a close second and third place.

Q15. You stated losing money or personal/financial information in a deceit. What was the main reason this happened?

A world without fraud?

“Fraudsters will always use new tools and techniques to stay ahead of the game and gain people's trust.”

"Fraud is perpetrated as a combination of different Attack Vectors, targeting individuals or groups."

A world without fraud?

Malware

Bad faith

Phishing

Account Takeover

Mobile Sim Swap

Authorized Push Payment

Social engineering (app scams, impersonation, etc)

What is Artificial Intelligence?

What is Artificial Intelligence?

Artificial Intelligence (AI)

Artificial Intelligence **allows machines to accomplish tasks humans execute with intelligence**!

Machine Learning (ML)

Extraction of patterns from a historical dataset to generate insights and forecasting based on experience.

Deep Learning (DL)

Complex neural networks, inspired by the neurons of the human mind, and which can process a very large amount of unstructured data.

Generative AI (GenAI)

Generation of **contents** (text, multimedia, source code, etc.), usually from a text prompt describing the desired outcome.

Large Language Models (LLMs) GPT-like models

A specific type of GenAI models specialized in NLP and pretrained to generate **context-aware text contents** in a conversational way.

Technical fraud with AI

WORLDLINE

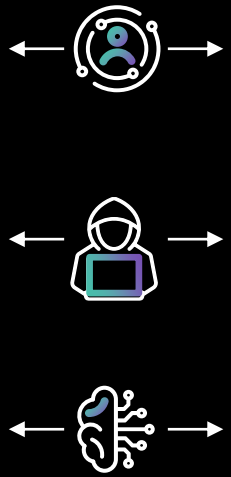
Fraud and AI – The challenges

Before

Card payment fraud was among the most reported forms of fraud, contributing significantly to overall financial losses

Account takeover incidents rose sharply before AI implementation, becoming one of the leading types of fraud.

Traditional fraud detection systems relied heavily on predefined rules and manual processes, leading to a high number of false positives



Now

Identify fraud attempts have surged by 80% over the past three years, highlighting the growing sophistication of fraud tactics.

Deepfakes now account for about 6.5% of total fraud attempts, asking a staggering increase of 2137% compared to three years ago. This indicates a shift toward more advanced methods of impersonation. *

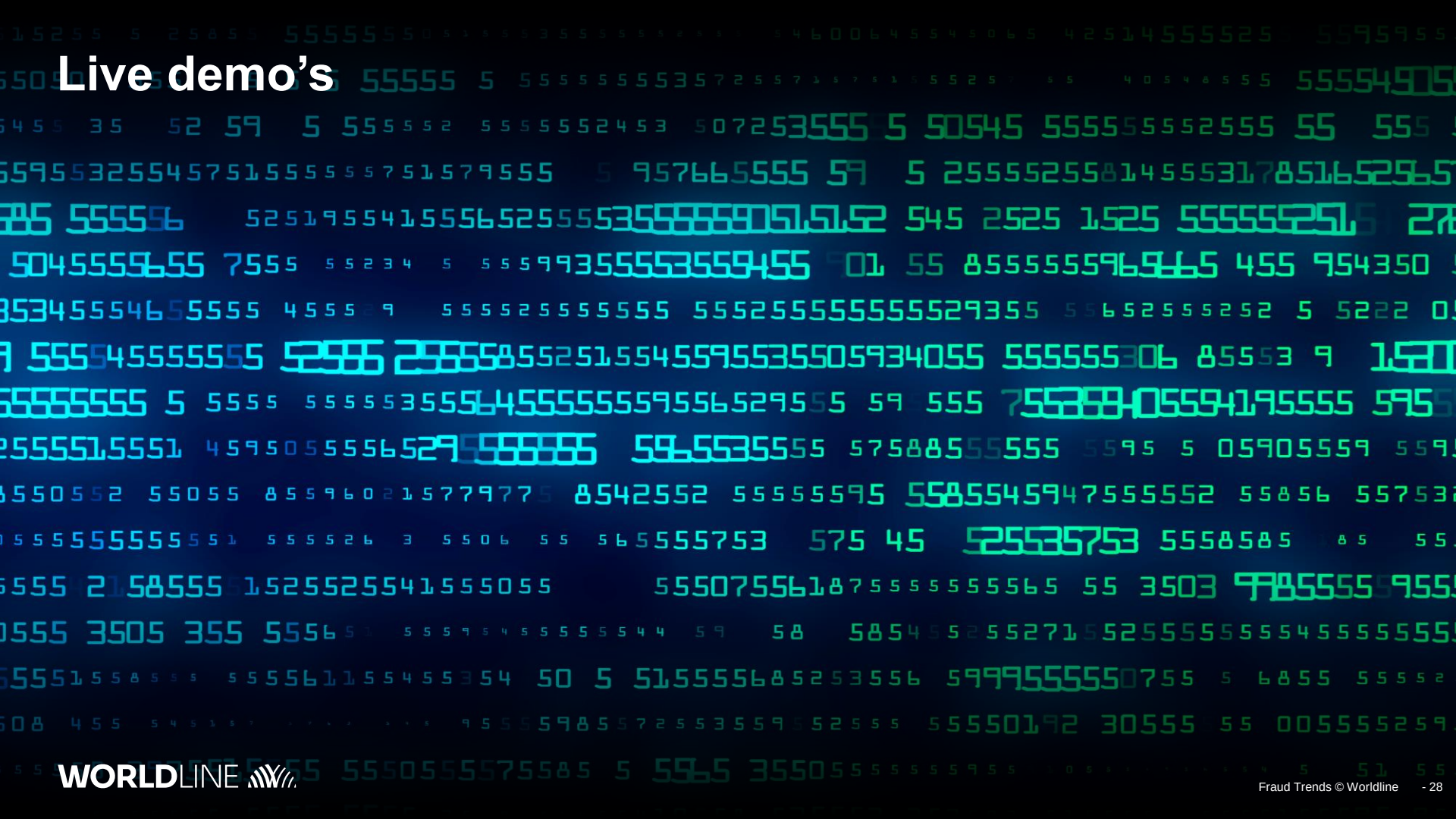
The financial impact from AI-driven fraud is notable, with institutions reporting that around 38% of their losses due to fraud are attributable to attacks using AI technologies.

** Source: ECB*

** Source: Brussels time*

WORLDLINE

Live demo’s



CEO Fraud

Audio deepfake

Solutions using AI to fight against frauds

WORLDLINE

Fraud & AI – The opportunities

Constant monitoring

Real-time processing

Increased accuracy

Rules creation

Embedded fraud management

Operational efficiency

Faster detection

Gain of time

Bridging fraud protection

WORLDLINE

Holistic Fraud Prevention

DIGITAL SECURITY SUITE

User & Device security

- Strong customer authentication & biometrics
- Security of devices & prevention of scammers
- E-commerce fraud prevention with 3D Secure

FRAUD MANAGEMENT SUITE

Transaction monitoring

- Real-time detection and action on high-risk transactions
- Continuous evolution of detection rules and AI models
- Fraud alert handling & case investigation

Device intelligence for a better fraud prevention

Advanced Data Collection

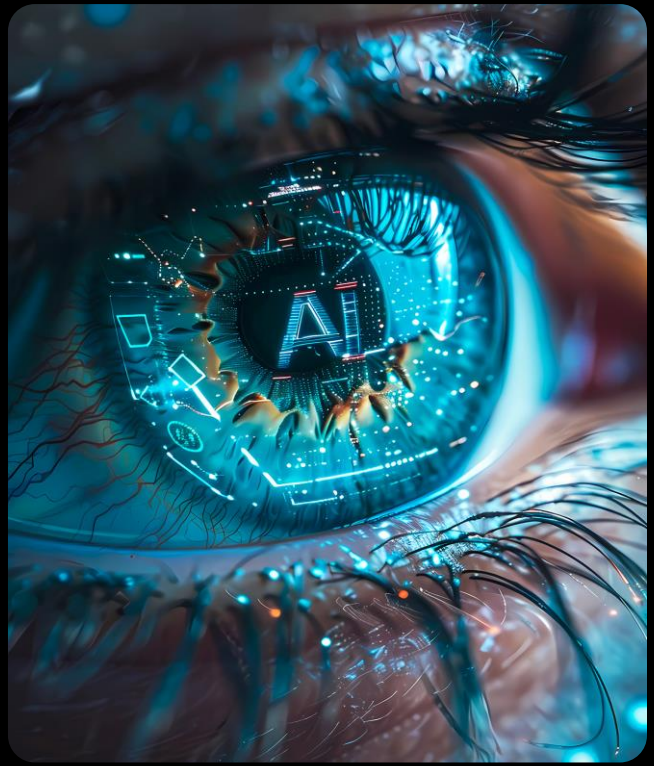
Collect information from devices

Mobile SDK

Web SDK (Javascript)

Collect information from external sources

- Eg. Telco operators (sim swapping, numer verify, ongoing call, etc.)
- Eg. Signal Spam database (mobile phone numbers + IP address)



Device Intelligence Scoring

Device Prevention Score (security compliancy)

Is the device at risk?

Is the device subject to a potential alteration / malware?

Device Imprint Score (device binding)

Do I recognise the device for this user?

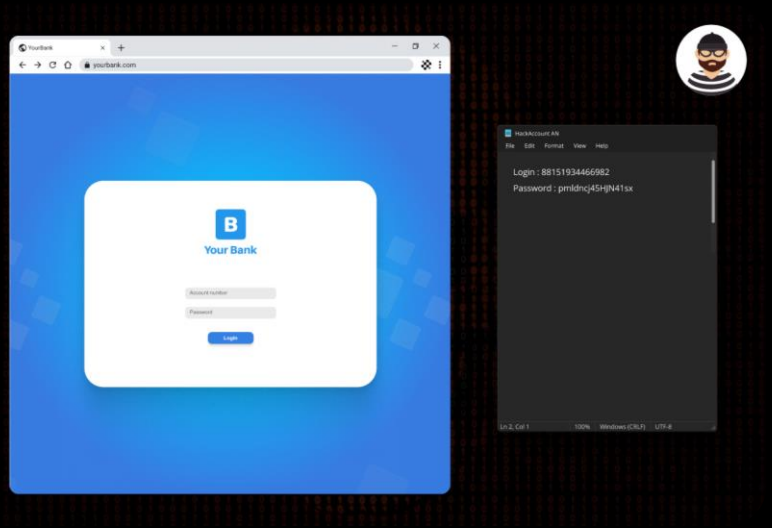
Do I recognise this device from the blacklist of devices?

User Behavioral

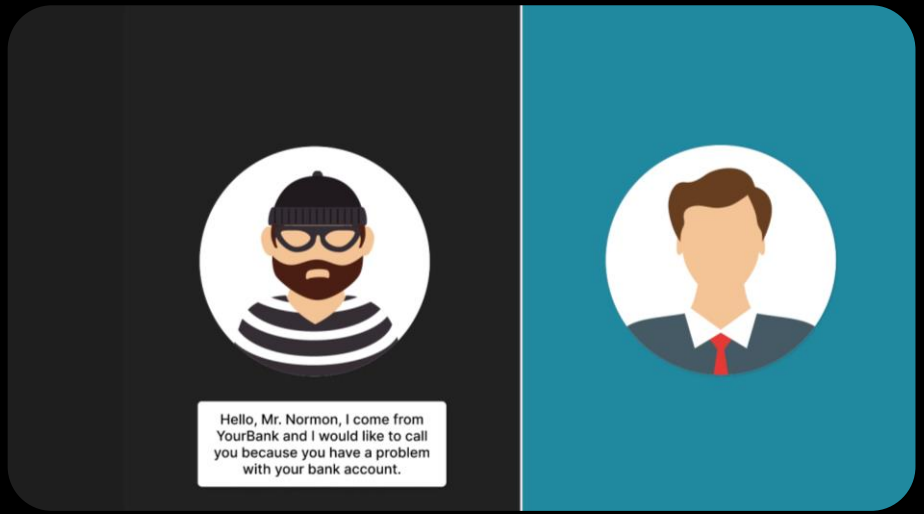
Do I recognise the behaviour of the user (way of holding the device, typing on keyboard, using mouse, ...) to prevent from phishing

Do I detect bot and emulation?

Device intelligence for a better fraud prevention



How DSS scores can prevent **phishing attack**?



How DSS scores can prevent **impersonation fraud**?

Some interesting figures

18B+
transactions analyzed per year

50M+
devices secured per month

+30%
improvement on fraud detection with AI

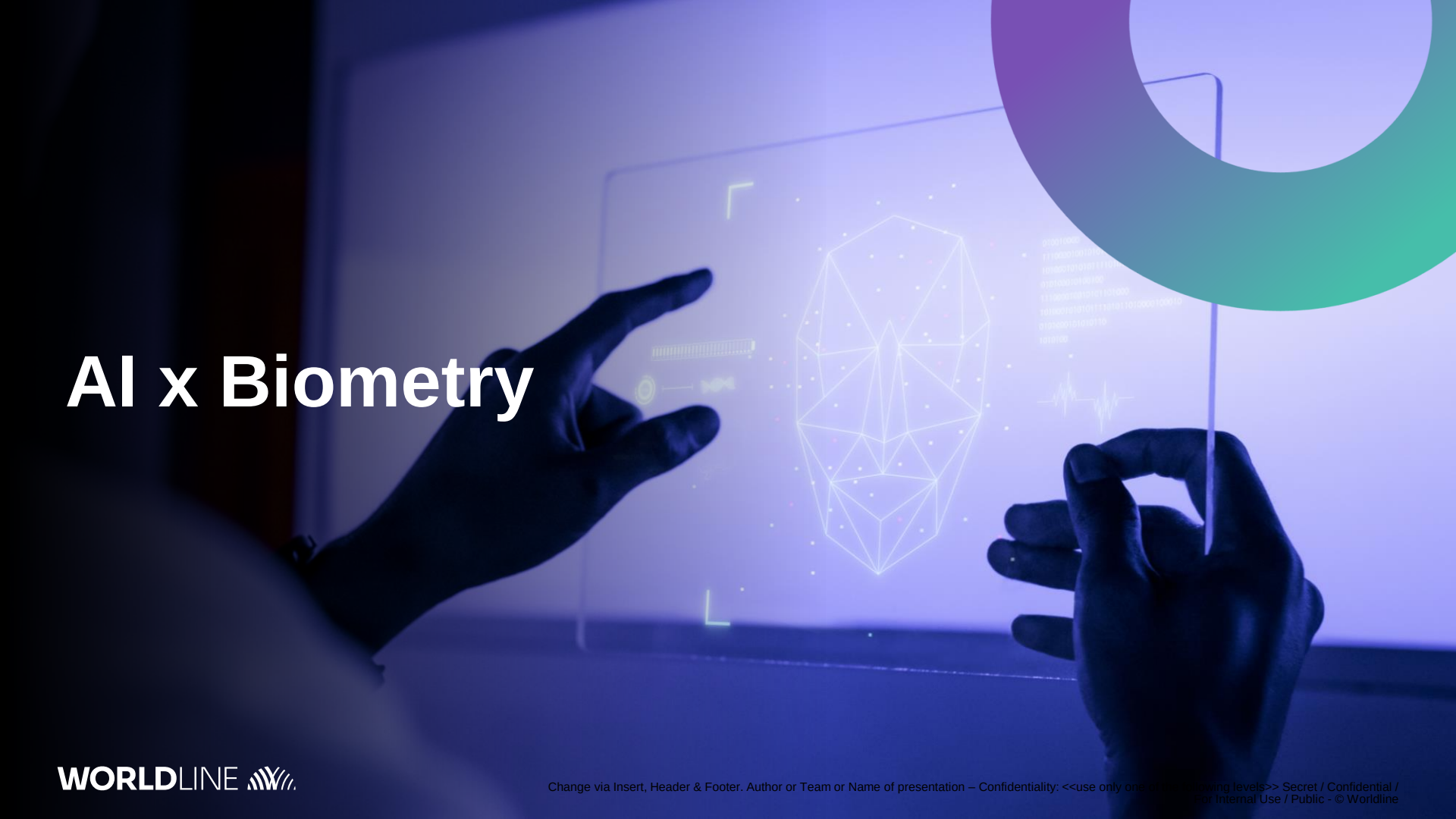
+85%
detection of false alerts

40 milliseconds
to detect if there is fraud or not

11 milliseconds
for AI to detect fraud in real time

AI applications in the payment industry

AI x Biometry



The future of payment

How AI x biometrics can transform Payment eXperience?

No cash, no card, no friction

Facial recognition

Click & Face Collect

In-car Payment

Multimodal & palm/vein payment

Multimodal & palm/vein payment

Voice biometry

Multi-device & online voice payment

Behavioral biometry

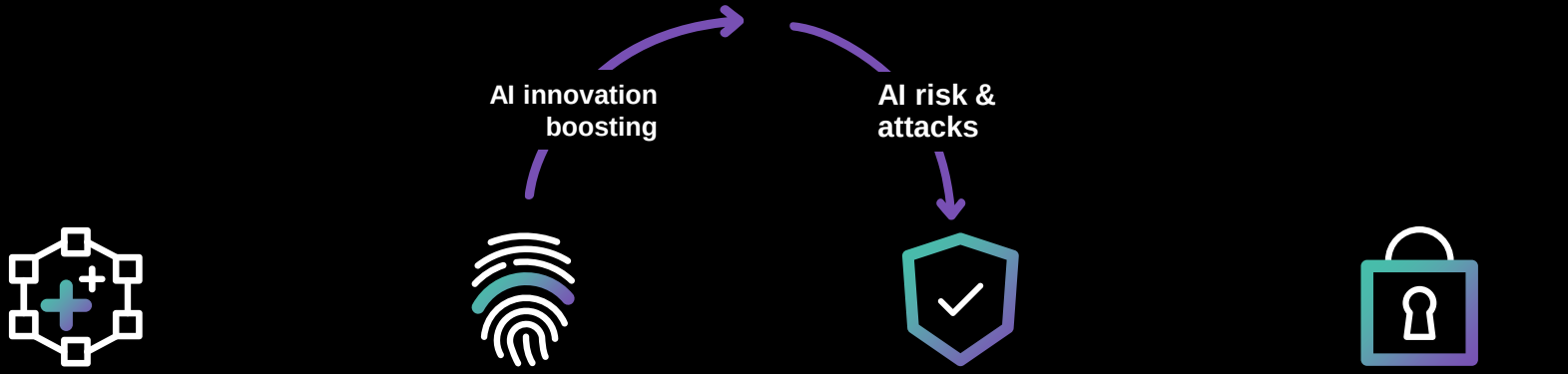
Continuous authentication

Behavioral biometry

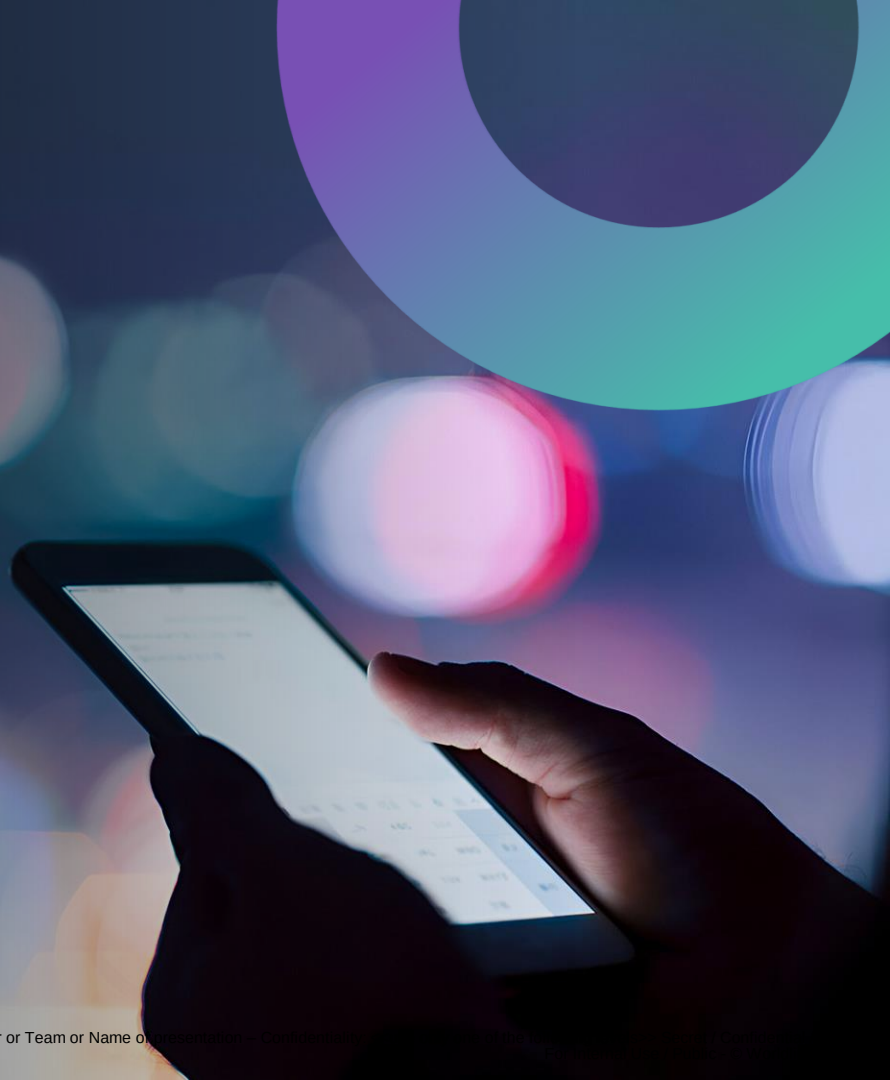
In game silent authentication

The future of payment

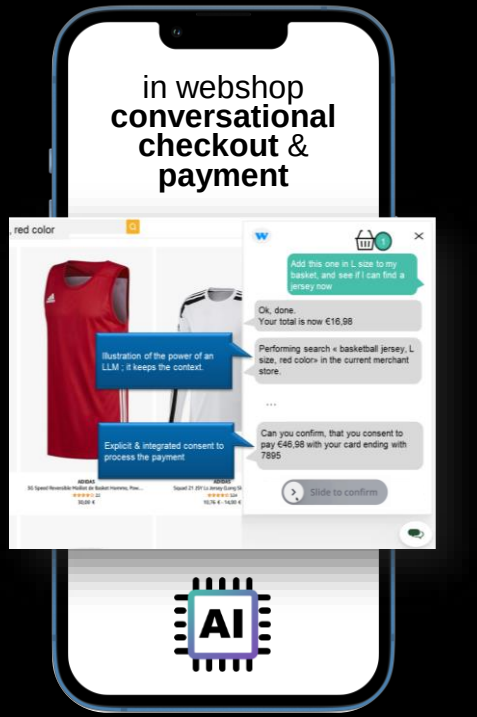
Biometrics challenges for Payment Xperience



Gen AI x e-shopping checkout payment



LLM-Checkout & LLM-Payment explorations



...

Thank you!

WORLDLINE