

# How Artificial Intelligence is reshaping the landscape of fraud?

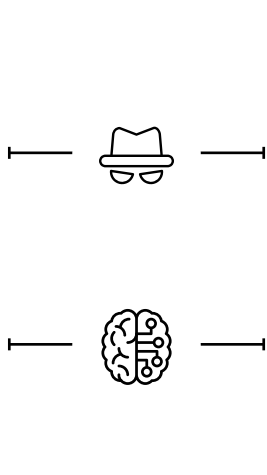


## Before

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

Identity 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, making 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

## Highlighting emerging fraud types fueled by AI.

### Phishing

#### What is it?

#### What is the role of AI?



The process of attempting to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity using bulk email, SMS text messaging, or by phone. The message will prod the victim into revealing sensitive information, clicking on links to malicious websites.

Phishing attempts have become more sophisticated. AI can create highly personalised messages that closely mimic legitimate sources, increasing the chances of victim engagement.

Additionally, AI automates content generation, enabling fraudsters to scale operations and target numerous individuals.

### Impersonation

#### What is it?

#### What is the role of AI?



Impersonation fraud is a type of deception where an individual pretends to be someone else to gain access to sensitive information or financial resources.

For example, when a fraudster misrepresents himself as a legitimate bank employee to urge the payer to issue a bank transfer.

Facilitated by AI and social engineering techniques, impersonation fraud can involve fake emails, phone calls, or even AI-generated voice mimicry.








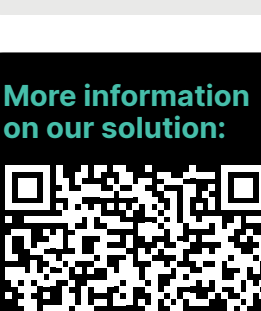
Attackers create a sense of urgency, playing on victims' emotions to lower their guard. The result is often financial loss and compromised personal data, making it a prevalent and dangerous form of fraud in today's digital landscape.

## Tackle new challenges with AI-driven security solution Digital Security Suite



In response to these challenges, Worldline has developed Digital Security Suite, offering a device intelligence solution based on AI and machine learning, specifically designed to combat fraud and identity theft for our customers. Our solution has the capability to protect all devices against various types of fraud during sensitive operations such as authentication, payment, and digitalization of sensitive use cases. Furthermore, our solution is built exclusively on device-based intelligence and does not depend on payment habits.

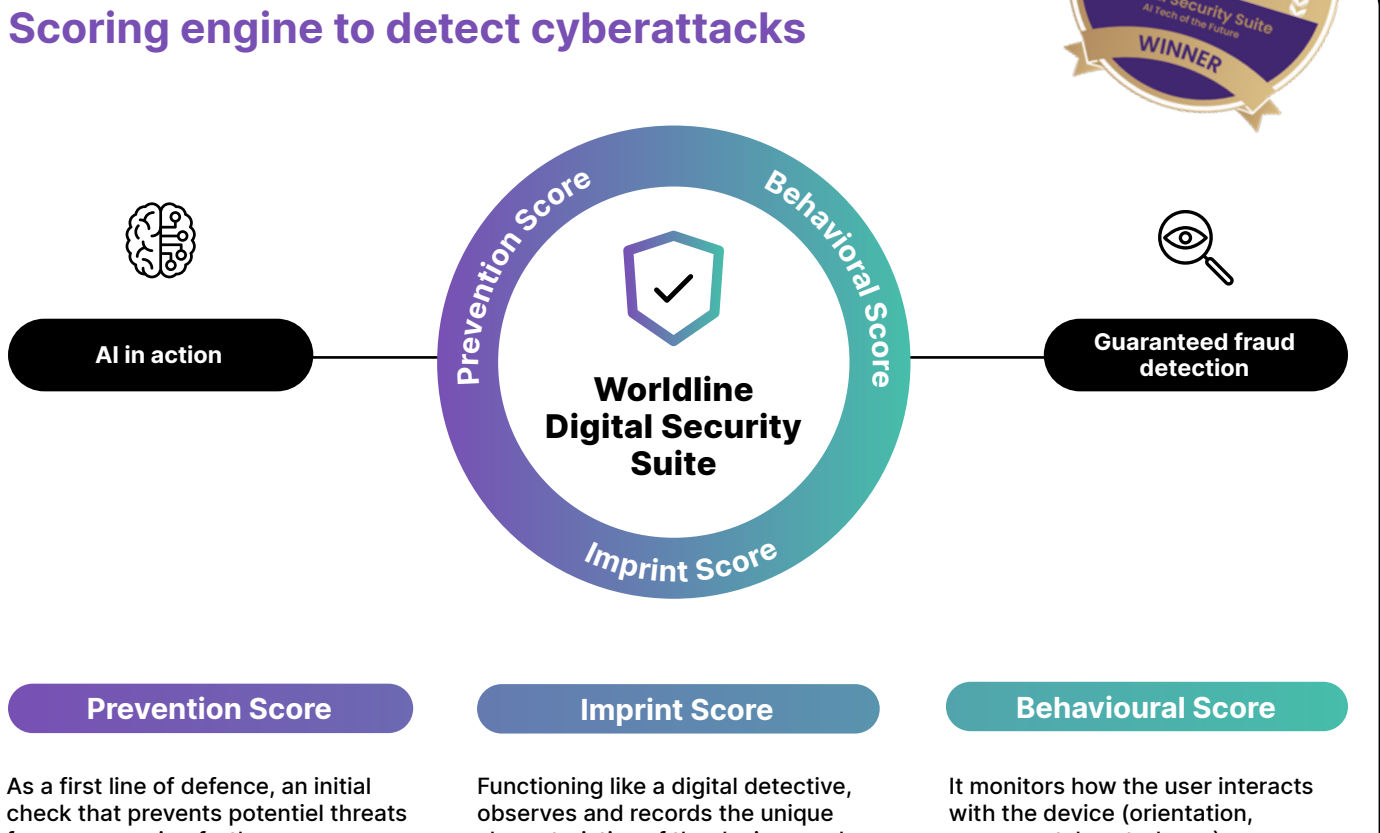
### All fraud risks are covered!

 <p><b>Malware</b> Any type of software designed to harm a computer system, disrupt its operations, steal information, gain control or cause other damage to data, devices or users.</p>	 <p><b>Bad faith</b> A payer who refuses to acknowledge that they have actually validated the transaction. The bank has 10 days to prove negligence or bad faith.</p>	 <p><b>Phishing</b> A payer who refuse to admit that they have actually validated the transaction. The bank has 10 days to prove negligence or bad faith.</p>	 <p><b>Account takeover</b> An unauthorised access and control of a user's account by an unauthorised individual or entry. This occurs when a malicious actor gains access to a person's login credentials.</p>
 <p><b>Mobile SIM Swap</b> Fraud technique that involves transferring a victim's phone number from their original SIM card to a new SIM card controlled by an attacker.</p>	 <p><b>Authorised push payment</b> A payer is misled into authorising a transfer of funds to a scammer or fraudster.</p>	 <p><b>Social engineering (app scams, impersonation, etc)</b> Tactic of manipulating, influencing, or deceiving a victim in order to steal personal and financial information.</p>	<p><b>More information on our solution:</b></p> 

### Utilising AI to protect your users' devices



#### Scoring engine to detect cyberattacks

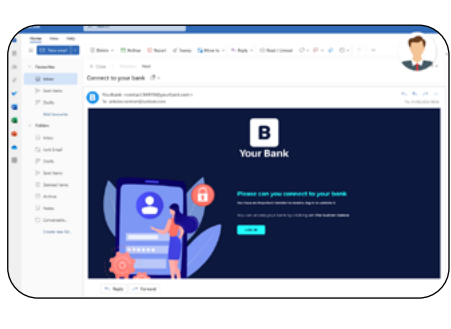


### How will our solution respond to concrete fraud use cases?

#### Phishing use case

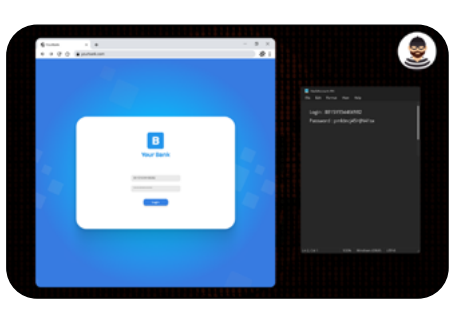
##### #1

The user receives a fake e-mail pretending to be his bank, he provides his credentials information.



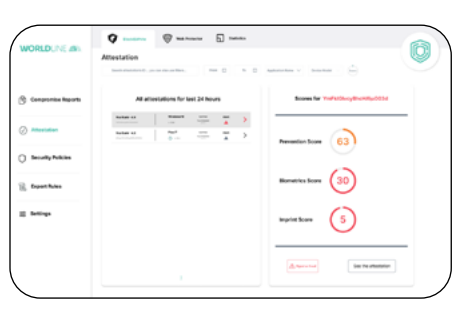
##### #2

The fraudster uses the user's credentials to connect to bank. He will be blocked in his attempt to connect.



##### #3

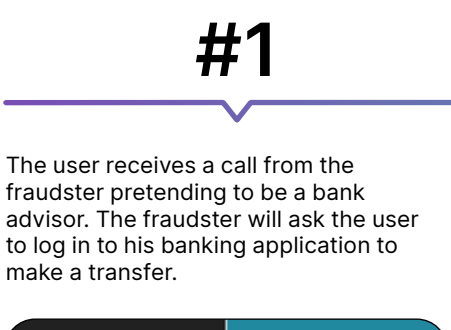
Why was he blocked? Because the Digital Security Suite scores indicated a high risk in biometrics and fingerprint, prompting an appropriate response.



#### Impersonation use case

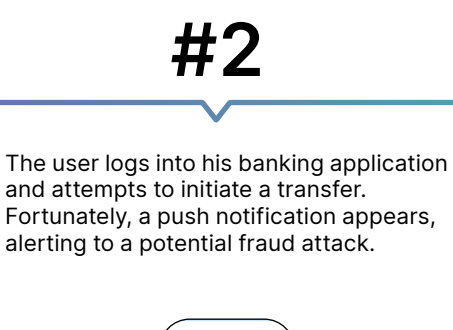
##### #1

The user receives a call from the fraudster pretending to be a bank advisor. The fraudster will ask the user to log in to his banking application to make a transfer.



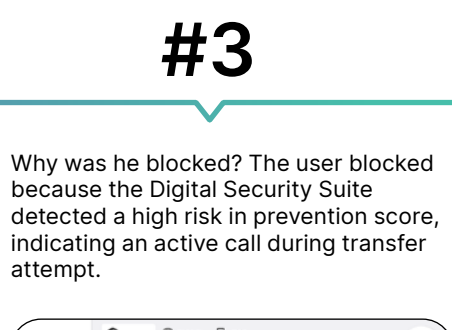
##### #2

The user logs into his banking application and attempts to initiate a transfer. Fortunately, a push notification appears, alerting to a potential fraud attack.



##### #3

Why was he blocked? The user blocked because the Digital Security Suite detected a high risk in biometrics and fingerprint, indicating an active call during transfer attempt.



### About Worldline

Worldline [Euronext: WLN] helps businesses of all shapes and sizes to accelerate their growth journey – quickly, simply, and securely. With advanced payments technology, local expertise and solutions customised for hundreds of markets and industries, Worldline powers the growth of over one million businesses around the world. Worldline generated a 4.6 billion euros revenue in 2023. [worldline.com](https://worldline.com)



For further information  
WL-marketing@worldline.com