Use Case

Stop Authorised Push Payment scams in their tracks

In 2022, Authorised Push Payment (APP) fraud losses in the UK alone amounted to £485.2 million, a stark indication of the growing threat and the importance of proactive fraud prevention.

Source - UK Finance

Cleafy's distinctive approach

- **Gain total control:** Achieve full visibility and control over your fraud risk management, enabling precise oversight at every stage.
- **Real-time threat response:** Detect and neutralise threats instantly, preventing financial losses before they impact your customers.
- **Stay ahead of fraud:** Leverage advanced predictive technologies to anticipate and outpace emerging fraud trends.
- **Cross-channel insight:** Access comprehensive visibility across all customer interactions, enabling precise, real-time decisions with near-zero false positives and negatives.
- **Advanced AI-driven analysis:** Utilise best-in-class AI and machine learning with our AI fraud assistant for immediate detection and mitigation of complex threats, even on zero-day attacks.

The rise of APP fraud and multi-channel threats

As instant payments and sophisticated **AI-driven deep fakes** evolve, the threat landscape has become increasingly complex. Cybercriminals exploit multiple channels—phone, video calls, SMS, email, and social media—to deceive victims and evade traditional security measures. **Reacting only at the point of transaction is often too late and risky.**

Key challenges:

Real-time transactions
The speed of instant payments leaves little room for error, complicating the reversal of fraudulent transactions.

Deep fake technology
Advanced AI can produce highly convincing fake audio and video, making scam detection increasingly difficult.

Multi-channel attacks
Scammers use various platforms to execute their frauds, necessitating a comprehensive security strategy.

Low-friction requirements
Balancing robust security with a seamless customer experience remains a critical challenge.

Cleafy's comprehensive defence against scams

Predictive AI analysis

Harness the power of AI and millions of data points to proactively identify potential fraud risks, even from previously unknown accounts.

Device telemetry

Monitor and correlate device activity to detect suspicious behavior, such as concurrent phone calls or video calls during transactions.

Behavioral analytics

Track deviations from genuine customer behavior to flag unusual activities that may indicate fraud.

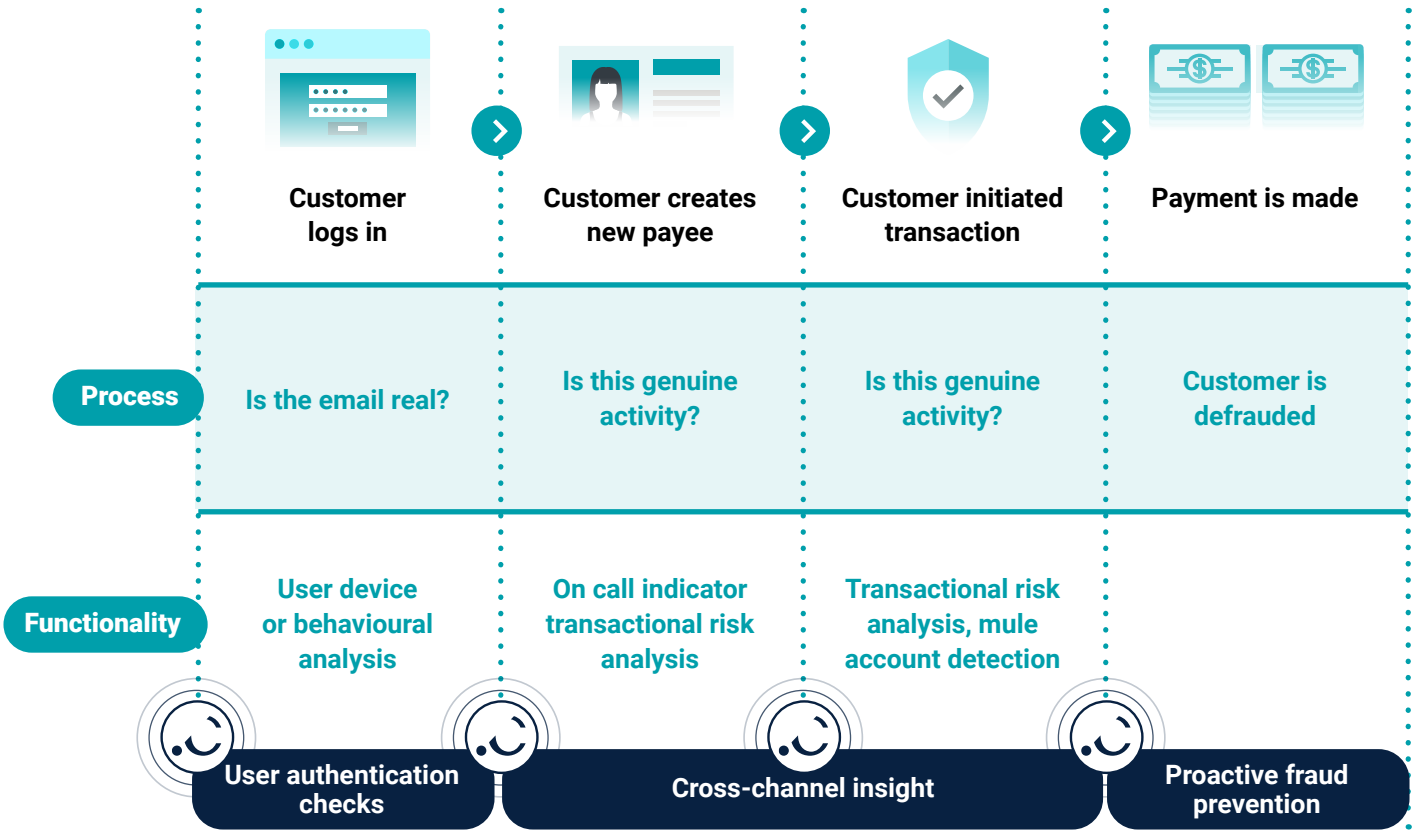
Real-time mule account detection

Utilise our continuously updated global database to identify and block mule accounts before they're used in fraudulent transactions.

Pattern-based real-time automation

Deploy smart rules driven by AI to detect and respond to fraud at scale with precision.

Always stay a step ahead with Cleafy



Facts, not aggregated scores: Understand the "why" behind every decision

Defend against the most sophisticated scams and fraud tactics.

1 What happened before the scam?

- **Was your customer/s targeted in a data breach?** Identify if any of your customers' personal information was compromised in a known breach.
- **Were there early signs of cyber threats?** Were there any indicators, such as phishing attempts or suspicious login attempts, that could have signaled a potential attack.

> "81% of fraud attacks include a combination of cyber and social engineering."

2 What were the key steps in the scam?

- **Were the customer's credentials tested or compromised?** Understand if their login information was probed or used in unauthorised access attempts.
- **Was malware involved in the attack?** Check if any malware was detected on the customer's device or within your systems that could have facilitated the scam.

> "42% of fraud attacks include some kind of advanced malware."

3 What else was happening?

- **Is this part of a larger, coordinated attack?** Assess if the scam is a component of a broader, multi-threaded attack targeting multiple customers or accounts.
- **Was there a cross-channel strategy used to exploit vulnerabilities?** Reveal if the attackers used multiple communication channels (e.g., email, SMS, phone) to increase their chances of success.

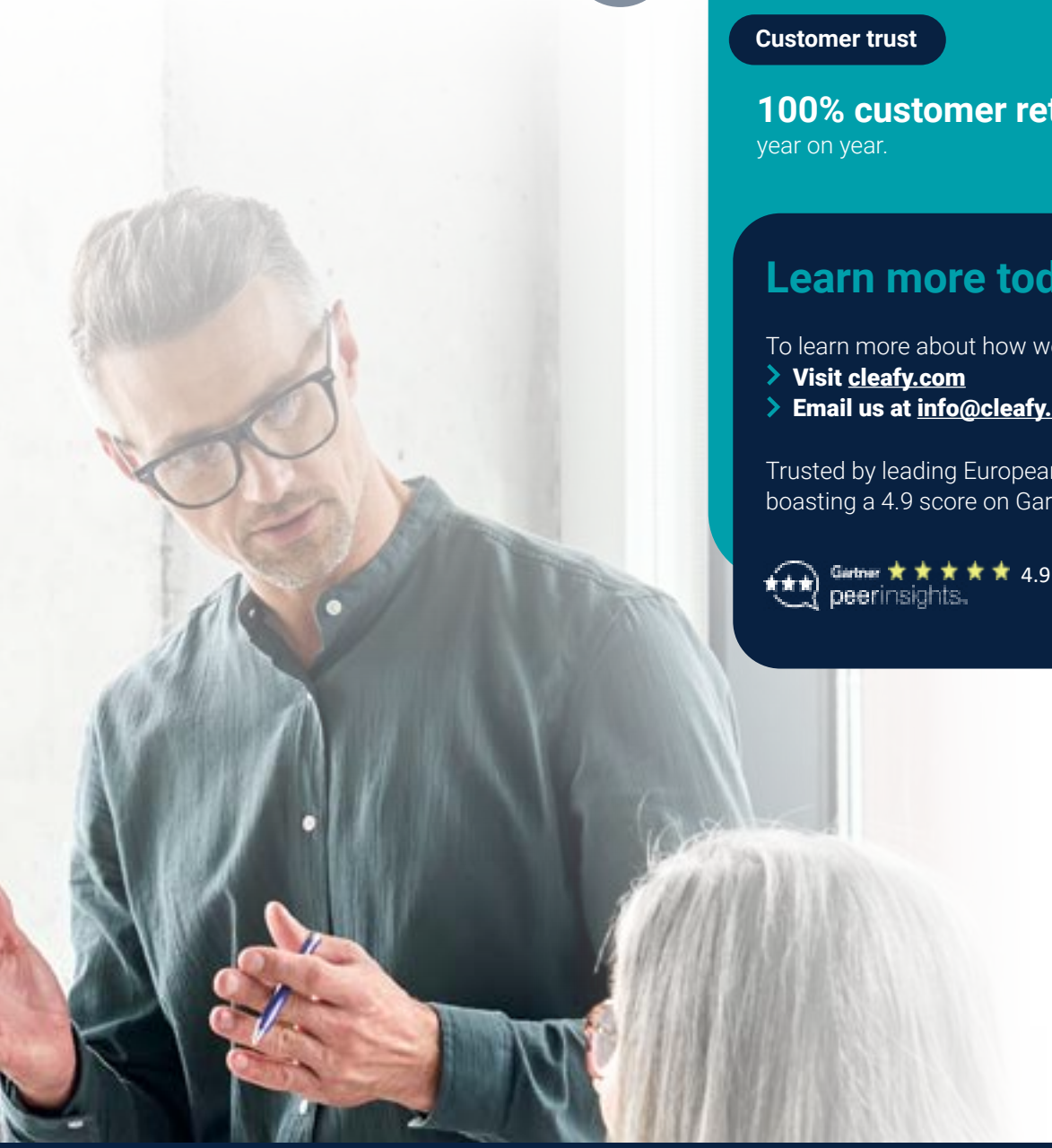
> "Often times, the social engineering attempt is not the only piece of the puzzle. Proactive monitoring to prevent scams."

Cleafy customers experience

97% reduction in unnecessary Strong Customer Authentication (SCA) requests and blocked transactions, enhancing the customer experience.

89% decrease in unresolved or active fraud cases, easing analysts' workload and boosting operational efficiency.

91% drop in attacks, resulting in significant financial savings.



Protecting against tomorrow's threats today

Global presence

Cleafy secures billions of transactions from over **100 million accounts globally.**

Innovation

79 technology patents and ongoing advancements.

Customer trust

100% customer retention year on year.

Learn more today

To learn more about how we can help you,

- **Visit cleafy.com**
- **Email us at info@cleafy.com**

Trusted by leading European and LATAM banks, boasting a 4.9 score on Gartner Peer Reviews.

Gartner peerinsights. ★★★★★ 4.9