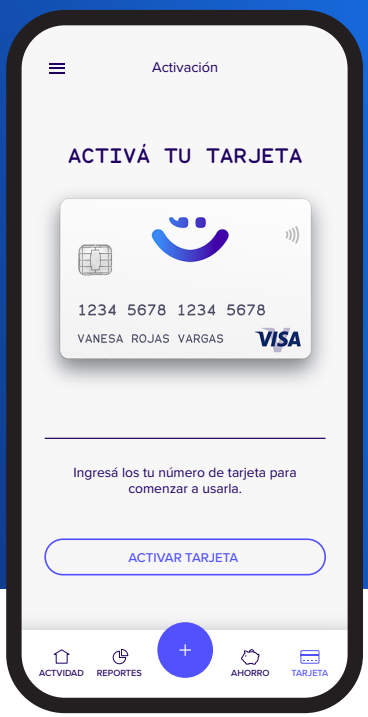
SHIELD | WINK

Case Study

Building Trust in Fintech: How SHIELD Empowers WINK to Fight Fraud and Drive Growth?



Key Takeaways

Over **99.9%** genuine user rate

Solidified trust in the platform

Prevent account takeovers from accessibility permission exploits

WINK's journey to ensuring a secure and reliable platform

The WINK app allows customers to easily open savings accounts within 5 minutes, make mobile purchases and payments, organize their finances, as well as categorize and group expenses.The fintech brand's promise is to provide agile, queue-free, user-friendly, and reliable financial services, without the need for customers to visit physical branches.

WINK wants to ensure security and trust in a service that is 100% digital. Fraud is always top-of-mind for fintech platforms, as they are concerned that fraudsters will **abuse platform promotions, steal user's funds** or **launder money**.

That's why WINK chose to use SHIELD Device Intelligence. The cutting-edge AI-powered technology enables the WINK team to stop fraud in real time, stay ahead of risks and build trust in their ecosystem.

Customer Profile

Founded in 2018, WINK is the first neo cooperative in Costa Rica and the first app to offer completely digital financial services in the country, eliminating the need for customers to visit physical branches. It's owned by Coopenae, a cooperative with over 50 years of history.

Industry

Financial Services

Region

LATAM

A deep dive in how fraud occurs in the fintech industry

Fraudsters use a variety of tactics to launch **promo abuse**, **account takeover** and **money laundering** attacks towards the fintech industry.

They employ tools including app cloners and emulators to create thousands of **fake accounts**. They can then conduct promo abuse - for example, using these accounts to exploit lucky draws and limited offers. This artificial inflation of user numbers and activities can deceive the platform into believing that it is experiencing genuine user growth and engagement.

Account takeovers (ATOs) are also a pervasive threat faced by the fintech industry. Fraudsters are constantly trying to gain access to users' accounts to steal their money or make unauthorized transfers. To achieve this, their tactics include **abusing accessibility permissions**, as well as the use of **malware** and **malicious tools**. Cybercriminals can coerce users into downloading malicious apps. This, for instance, allows them to discreetly enable screen sharing and autoclickers. Such tactics simplify the process for fraudsters to exploit individuals, extract funds, and gain control over their accounts.

Malicious software facilitates another fraudulent technique, which involves generating **overlay screens** upon launching official banking apps. These deceptive overlay screens mimic the appearance of the legitimate banking app's interface but are, in fact, components of a different app. Consequently, users may unknowingly input their account credentials into the fraudulent overlay interface instead of the authentic banking app, providing fraudsters with unauthorized access to their accounts.

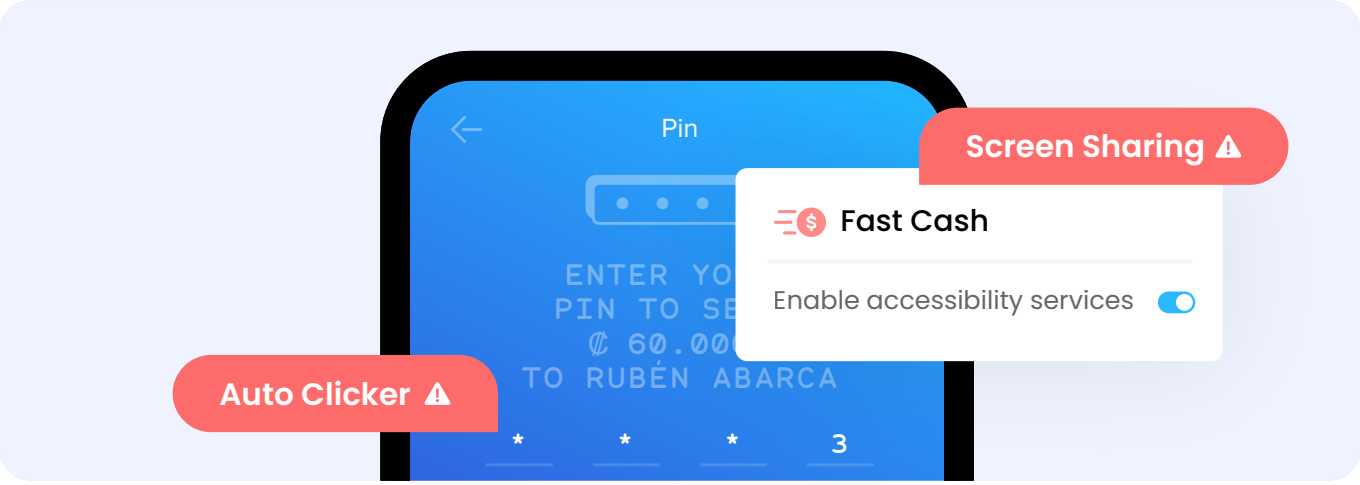
Money laundering is another big issue. Illicit fund transfers, when done across tens of thousands of fake accounts, are exponentially more difficult to trace. Criminals can also use compromised user accounts to do so.

Fortifying the security of WINK platform with SHIELD

WINK knew they needed powerful technology to fortify the security of their platform and operations. So they partnered with SHIELD to stop all fraud threats on its platform.

> ***"The partnership with SHIELD has proven crucial as it detects fraud attempts in real-time, empowering WINK to build trust with our users."***

Diego Loaiza
Director, WINK



They leverage **SHIELD Device Intelligence** to help them guarantee a fraud free ecosystem. The technology is used to continuously monitor tens of thousands of device, network, and behavioral data points in real time in order to create a complete picture of risk. No Personal Identifiable Information (PII) is required, and it prioritizes privacy while fully complying with general regulations.

SHIELD Device ID, the global standard for device identification, supported them in identifying fraudulent devices used to create fake accounts, preventing **promo abuse**. The feature also empowered WINK to trace links between fraudulent accounts and devices, bolstering the company's **Anti-Money Laundering** capabilities.

The team further harnessed the **SHIELD Risk Intelligence**, identifying malware and malicious tools associated with fraud, such as app cloners, autoclickers and emulators - thus addressing the issue of fraudsters **exploiting accessibility permissions to conduct account takeovers**.

Device Intelligence also helps them to efficiently onboard new customers and pinpoint devices displaying potentially fraudulent activity, stopping fraudsters before they can even join the platform. This allows the WINK team to focus on users that are legitimate, without the need to implement extra manual reviews or other security measures that could negatively impact the user experience.

SHIELD's technology empowers them with actionable real time device intelligence. The result is an optimization of the team's time, the elimination of fraud, the fortification of a trustworthy ecosystem and the growth of legitimate users.

"The partnership with SHIELD has proven crucial as it detects fraud attempts in real-time, empowering WINK to build trust with our users", commented Diego Loaiza, director at WINK.

SHIELD is a device-first risk intelligence company. We are dedicated to helping organizations worldwide eliminate fake accounts and all malicious activity with the global standard for identification and intelligence.

Leveraging AI, we identify the root of fraud and provide actionable risk signals in real time, helping all online businesses stop fraud, build trust, and drive growth.

With offices in San Francisco, Miami, London, Berlin, Jakarta, Bengaluru, Beijing, and Singapore, we are rapidly achieving our mission - eliminating unfairness to enable trust for the world.

For more information, visit **shield.com**.

/shieldfraud

/shieldfraud

/company/shield

shield.com