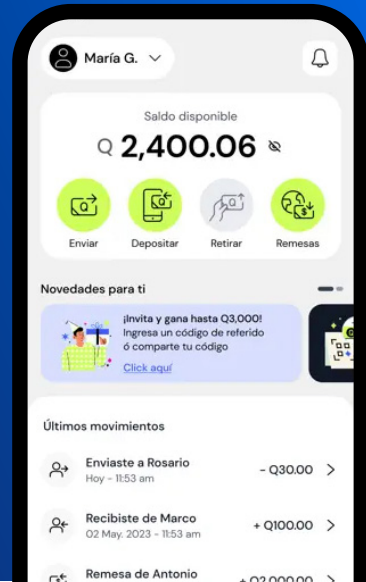


Case Study

# SHIELD Secures Zigi Financial Services App & Its Users Against Fraud



“SHIELD’s technology empowers us to stay ahead of fraudulent activities, ensuring the highest standards of security for our ecosystem and customers.”

**Brenda Menjivar**  
Chief Data Officer, Zigi App

## Key Takeaways



Eliminated fake accounts abusing promotions



Prevented account takeover attacks, protecting users’ accounts



Ensured a trustworthy ecosystem

## Enabling users to manage their finance in a simple and secure way

The Zigi platform helps Guatemalans manage their finances by allowing them to receive remittance, send money, pay offline with a QR code and more. Zigi’s mission is to help people grow their wealth as well as accelerate financial inclusion throughout Central America.

Security is their top priority. Despite the prevalence of fraud in fintech solutions that can undermine user trust, Zigi is proactively addressing the risks posed by cybercriminals. They have opted for **SHIELD’s device-first risk intelligence solution** to detect and stop fraud at the root, protecting their customers and the overall ecosystem.

### Customer Profile

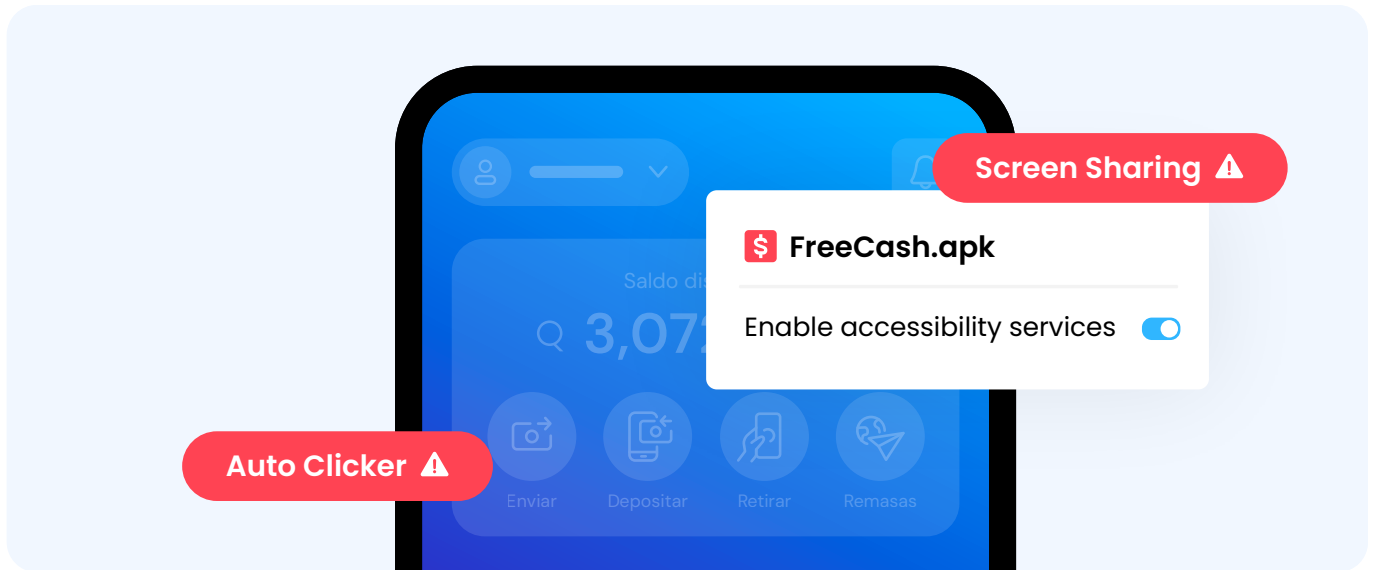
Zigi is a fully digital financial services app based in Guatemala. The platform caters to the population’s essential financial needs, enabling users to manage their money in a simple, transparent, secure and accessible way.

### Industry

Financial Services

### Region

LATAM



## Account takeover attacks are on the rise

**Account Takeover (ATO)** attacks are on the rise and the financial industry is a primary target for cybercriminals. The term refers to fraudsters illicitly accessing and taking control of users' bank accounts to perform unauthorized transactions, transfer funds, or engage in other malicious activities.

Fraudsters typically use **social engineering tactics** to carry out ATO attacks, wherein fraudsters manipulate users to expose login data or download malware. **Phishing** or **spear-phishing** is an example of this type of threat. In such attacks, criminals send messages or emails that appear to be from legitimate sources, such as banks or trusted organizations. These messages often contain links to fake websites/apps created to collect confidential information or to trick the user into installing malware.

Fraudsters also exploit **accessibility permissions** to perform ATO. Cybercriminals can manipulate users into downloading **malicious apps** and subsequently granting accessibility permissions to those apps. For example, fraudsters could then activate **screen sharing** and **autoclickers** without the victim's knowledge. These make it easier for fraudsters to manipulate customers, take over their accounts and extract their money.

## Mitigating Promo Abuse Fraud in the fintech industry

Zigi offers users discounts when they pay using the app and also provides a referral program that encourages existing customers to recommend the platform to friends and family.

These promotions usually attract fraudsters that employ malicious apps and tools, including **app cloners** and **emulators**, to create thousands of fake accounts. These accounts are then used to exploit platform incentives and promotions.

As a result, the platform's marketing budget can be wasted on fraudsters instead of rewarding genuine consumers and attracting new users.

## How SHIELD fortifies Zigi's Defense Against Fraud

The Zigi team knew that protecting the banking app from promo abuse and its customers' accounts from account takeover attacks were crucial to earning their trust. That's why they chose to use SHIELD's technology as the platform's first line of defense against fraud.

SHIELD's device-first risk intelligence solution is powered by cutting-edge device fingerprinting and the latest in AI & machine learning algorithms.



It identifies fraud at its root and analyzes thousands of devices, network, and behavioral data points to provide actionable insights in real time.

**SHIELD Device ID**, the global standard for device identification, enabled them to pinpoint the fraudulent devices used to create fake accounts, preventing **promo abuse** and **account takeover**.

The team further harnessed the **SHIELD Risk Intelligence**, identifying **malware and malicious tools** associated with fraud, such as **app cloners**, **autoclickers** and **emulators**.

SHIELD Risk Intelligence also ensures that the platform stays ahead of fraudsters with the Global Intelligence

**Network**: a continuously updated library containing all fraud patterns encountered, as well as the latest malicious techniques. With over 7 billion devices and more than 1 billion user accounts analyzed worldwide, SHIELD leverages this intelligence to synchronize real-time attack patterns.

The solution empowers Zigi team with actionable real time device intelligence and a proactive approach to fraud prevention, ensuring a secure and trustworthy ecosystem.

Brenda Menjívar, Chief Data Officer at Zigi said: "SHIELD's technology empowers us to stay ahead of fraudulent activities, ensuring the highest standards of security for our ecosystem and customers".

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](https://shield.com).

 /shieldfraud

 /shieldfraud

 /company/shield

 shield.com

