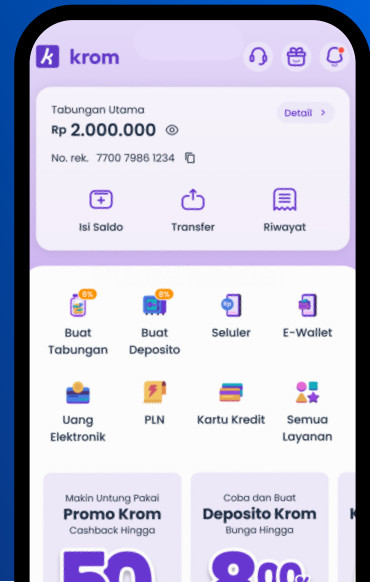


## Case Study

# Krom Bank Enhances Account Takeover Detection by 10x While Preserving Privacy-Secure Banking



“As Krom Bank encountered more sophisticated, AI-driven fraud, it became clear that static app hardening alone was no longer sufficient. While these controls protect app integrity, they offer limited visibility into live sessions and struggle to detect evolving, next-generation threats such as deepfakes. SHIELD acts as an essential layer of defense, providing continuous, run-time device intelligence, enabling Krom Bank to identify and stop advanced fraud tools the moment they are activated, without compromising user experience or privacy.”

**Alie Tan**  
Co-founder & CTO, Krom Bank

## Key Takeaways



**100%** of screen sharing attempts detected in real time



**10x** increase in Account Takeover (ATO) detection



**95%** improvement in overall fraud response time

## The Hidden Liabilities of Fraud

Krom Bank was founded to make banking simpler, faster, and more convenient for Indonesia's next generation of customers. But as digital adoption accelerates, fraudsters are exploiting this shift with increasingly sophisticated scams.

One of the most pressing threats comes from account takeover (ATO) attacks driven by social engineering and phishing. Fraudsters distribute fake or malicious apps that impersonate trusted institutions or widely used digital services, tricking customers into installing them on their devices. Once installed, these apps prompt users to log in to their bank accounts, giving attackers the opportunity to hijack live sessions using screen sharing and remote access tools.

In Indonesia, this tactic has surfaced in multiple forms, including counterfeit versions of widely recognized digital identity and government-related applications, such as Identitas Kependudukan Digital (IKD). Similar patterns have also been observed with other fake public-service apps, underscoring how attackers leverage familiar brands and services to gain user trust.

More recently, fraud rings have adopted AI-powered techniques like deepfakes, highly realistic synthetic audio or video that impersonates bank representatives, government officials, or even family members. By using deepfakes to gain trust

### Customer Profile

PT Krom Bank Indonesia Tbk, a subsidiary of Kredivo Group, is a licensed Indonesian bank regulated by OJK, the Indonesian Financial Services Authority.

With a vision to be the nation's most innovative digital technology-based bank, Krom serves retail and MSME customers with fast, safe, and accessible solutions built on trust and transparency.

### Industry

Digital Banking & Financial Services

### Region

Indonesia

and urgency, fraudsters make victims more likely to comply with instructions that ultimately expose their accounts to takeover attempts.

## Capital Gains in Security

As fraud tactics became more complex, Krom Bank placed greater emphasis on visibility into what happens during an active user session. App hardening solutions protect the app's code against tampering and reverse engineering, through code obfuscation and integrity checks, but their protections are inherently static.

Krom Bank found that this approach creates blind spots as fraud tools become more sophisticated. Many modern attack techniques operate dynamically during a live session, executing malicious actions in ways that evade static protections. These tools are often designed with stealth capabilities that deliberately conceal their presence and bypass traditional hardening measures.

To close this security gap, Krom Bank strengthened its defense with SHIELD's device-first fraud intelligence. Unlike static app hardening, which focuses on code integrity, SHIELD is deeply rooted in continuous, run-time visibility into device behavior. This allows Krom Bank to detect sophisticated next-generation fraud tools (such as deepfakes, screen sharing, remote access software, and other AI-enabled social engineering) and bypass techniques the moment they activate, ensuring protection throughout the entire user session.

SHIELD combines two core capabilities that work together to deliver unmatched accuracy and real-time protection:

- **SHIELD Device ID:** the global standard for device identification, uniquely and persistently identifying every physical device with over 99.99% accuracy. Even if fraudsters attempt factory resets or app cloning, the SHIELD Device ID continues to identify the same device, eliminating fake accounts and preventing device cycling.
- **SHIELD Fraud Intelligence:** a layer of real-time, actionable signals that continuously profiles every device session. It enriches Krom Bank's existing risk models with 20+ risk indicators, providing deeper context for every interaction. This

enables Krom Bank to detect every malicious tool and technique the moment it is activated, such as when screen sharing is enabled or when a device shows signs of remote hijacking.

SHIELD achieves all of this without collecting personally identifiable information or sensitive identity data, ensuring Krom Bank's fraud prevention remains fully compliant with data privacy requirements under OJK oversight.

With SHIELD embedded into its fraud prevention framework, Krom Bank has moved from reactive to real-time defense:

- **10X increase in ATO detection:** By shifting from static protections to continuous device-level intelligence, Krom Bank now catches account takeover attempts that previously went undetected, including those driven by screen sharing, remote access, and deepfake-assisted social engineering.
- **100% of screen sharing attempts detected:** Every instance of screen sharing activation is now identified in real time, enabling Krom Bank to intervene before a session is compromised.
- **95% improvement in fraud response time:** Real-time risk signals allow Krom Bank's fraud team to act on threats as they emerge rather than investigating after the damage is done. Threats are neutralized silently in the background, without disrupting legitimate customers.
- **Account sharing fraud eliminated:** SHIELD Device ID enables Krom Bank to detect when a single account is accessed across multiple devices, or when one device operates multiple accounts.

## Delivering Safe and Seamless Banking

With SHIELD, Krom Bank has strengthened its defense strategy, eliminating blind spots against advanced scams while preserving a seamless user experience. Customers benefit from frictionless yet secure banking, while the bank reinforces its reputation as a trusted, forward-looking financial partner.

As Krom Bank continues its mission to become Indonesia's most innovative digital bank, SHIELD provides the intelligence and resilience needed to stay ahead of evolving threats, ensuring growth that is secure, sustainable, and privacy-preserving.

SHIELD is a device-first fraud intelligence platform built on the world's most persistent device identification technology across applications and platforms.

Powered by SHIELD AI and patented technology (SHIELD Sentinel), SHIELD sets the global standard for device identification (SHIELD Device ID) and exposes the full range of fraud tools and techniques through more than 20 risk indicators, delivering real-time, actionable fraud intelligence across all use cases and industries worldwide.

Trusted by global unicorns including inDrive, Alibaba, Deliveroo, Meesho, TrueMoney, Unico ID and OLX, SHIELD operates with teams across Los Angeles, São Paulo, London, Berlin, Jakarta, Bangkok, Bengaluru, Beijing and Singapore, advancing our mission: to eliminate unfairness and enable trust for the world.

For more information, visit [shield.com](https://shield.com).

 /shieldfraud

 /shieldfraud

 /company/shield

 [shield.com](https://shield.com)

