How risk management helps financial institutions (FIs) mitigate fraud and improve customer experience for digital banking

The pandemic changed our habits and digital banking is on the rise

- 4.2bn online banking users by 2026 from 2.5bn in 2021
- 82% of consumers who used online or mobile banking for the first time plan to continue to use this channel

82% of consumers who used online or mobile banking for the first time plan to continue to use this channel.

PROBLEM

- 15% increase in fraud attacks in 2021
- $1.551 average identity fraud cost in 2021, $256 higher than 2019
- 35% will cancel or delete an account or app if they have trouble accessing it

PROBLEM

- 23% increase in sophisticated automated attacks in H1 2021
- 14% of all attacks imitate human behaviour and evade standard bot-detection tools
- One attack can include hundreds of thousands to millions of access attempts

SOLUTION

Device intelligence lets you recognise legitimate users and detect anomalies in the network and devices.

- 85% of online traffic for FIs comes from a trusted user and
- 97% of fraud attempts are made on an anomalous device or network

SOLUTION

Behavioural biometrics and analytics analyses how a user types, holds the device, fills in forms and what their usual habits are...

- This differentiates ‘good users’ from fraudulent users and stop the most sophisticated automated bot attacks.
- User experience is improved with silent frictionless authentication of your ‘good users’

SOLUTION

Trust consortium monitors over 2bn events every month. It gathers anonymised and encrypted insights from online events across all our clients, and flags if an IP or device ID is linked to past fraud in another environment.

- 66% of attacks in 2020 had bad-reputation IPs, which were flagged.

RISK MANAGEMENT TECHNOLOGIES

Real-life usage

The following customer case studies reveal how the risk management technologies that power the Gemalto IdCloud platform have mitigated fraud during customer onboarding and daily access.

**Case 1**

Stopping application fraud (Onboarding)

- **Client:** US neobank
- **Problem:** Marketing campaign attracted fraudsters who tried to benefit from new account opening incentive, constantly modifying how they tried to bypass the digital onboarding security features.

- **SOLUTION:** Our fraud experts uncovered fraud patterns and implemented countermeasures based on fraudulent risk signals, blocking all attacks.

**An increasing problem:** New application fraud losses are expected to cost FIs in the U.S. $4.1bn by 2023 (+86% vs 2018).

**Case 2**

Stopping account takeover attacks (Access)

- **Client:** Major global bank
- **Problem:** Constant major advanced automated attacks that were bypassing current defence solution.

**SOLUTION:**

- Attacks involved thousands of logins per hour, using each IP address only up to five times a day. Within two weeks, millions of fraudulent attempts, missed by the previous solution, were stopped.

- 250m automated attacks mitigated
- >99% accuracy
- 0.1% false positives

For more information, visit thalesgroup.com