AIROME

COMPREHENSIVE FRAUD PROTECTION FOR ONLINE BANKING

GENERAL OVERVIEW

Modern banking infrastructure is developing in a high speed as well as the potential cyber threats which could cause the number of losses. Ensuring that digital banking users are always protected requires a complex of security measures and this should pass by seamless and unnoticeable for the client.

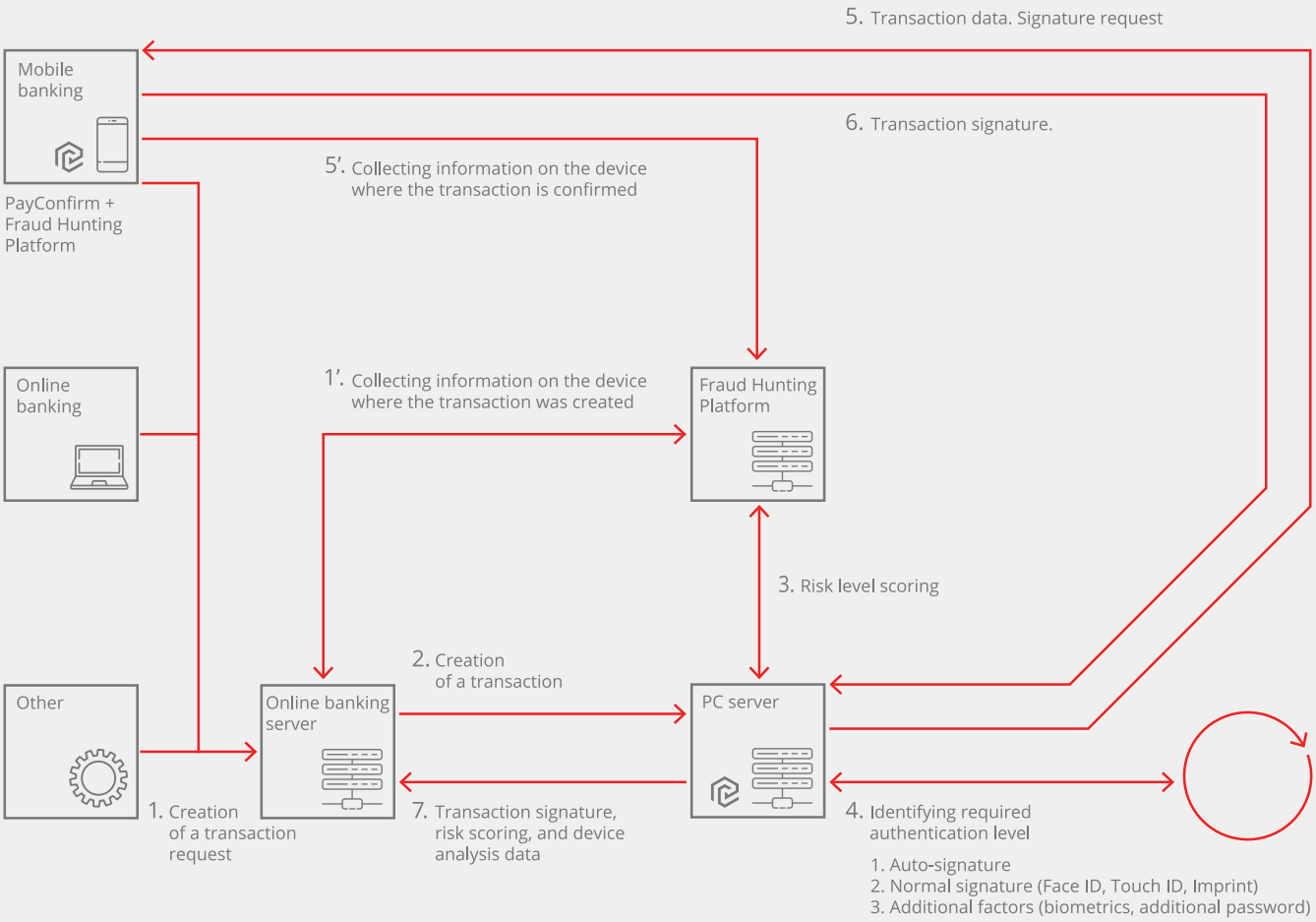
Adaptive authentication is the key to the smooth increase of security without any loss in client experience. To perform it in your bank, what you need is a proper authentication module bent with the anti-fraud one. With both modules onboard, you may differentiate those operations that need more attentions in terms of security and as a result request more attention from the client side. In case of potentially fraudulent activities detected on the client's smartphone — such as an attempt to confirm a money transfer from non-typical location, Trojan detected on the client's smartphone or any other suspicious behavior. In this case you may make a double check before transferring money: request to use biometry, secret code, etc.

The comprehensive module combines an anti-fraud platform and a mobile transaction authentication signature platform. This module is integrated into the mobile banking app installed on the user device.

With PayConfirm all the standard operations are confirmed with one tap on a smartphone screen. Wherever the operation was generated in mobile or internet bank, the client will receive a notification smartphone and the only thing requested is to tap "confirm" or "decline". Comparing to such methods of transaction confirmation as SMS, One-Time Password, scratch cards, MAC-tokens and others, PayConfirm makes the procedure more secure, user-friendly and cost effective for a bank.

Using behavioral analysis of user actions and device fingerprinting, the platform detects signs of fraud in real-time and identifies attempts to steal or use compromised credentials, banking Trojans, and web injections. The data collected is continuously stored and analyzed on server. At the same time, in case there is a regular transaction with low risk level — such as mobile operator purchase for example — then it may pass frictionless.

HOW IT WORKS



USER EXPERIENCE

For the Security department:

- Reduced number of bank fraud cases
- Detects the most popular cyber-attacks automatically
- Authentication based on asymmetric cryptography

For client:

- No need to keep and update your credentials or use SMS OTP
- Reduced time of confirmation
- Protects customers from financial fraud

ABOUT US

POWERED BY AIROME

airome.tech
info@airome.tech

POWERED BY GROUP IB

group-ib.com
info@group-ib.com