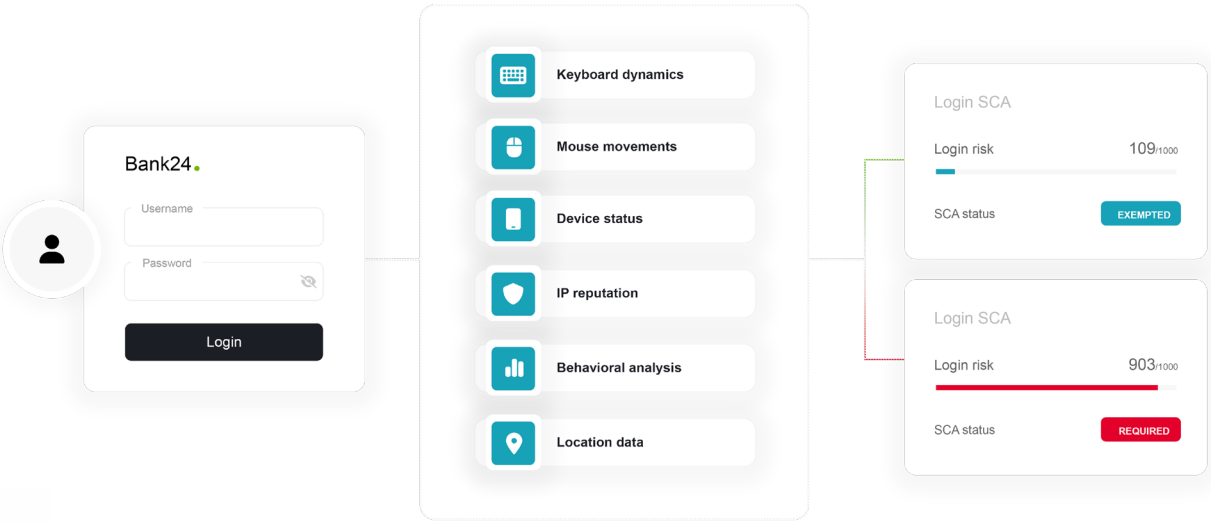
TRANSACTION RISK ANALYSIS.

Modern scam techniques have evolved.

PSD2, within the European Union, has been updated to improve payment security by incorporating Transaction Risk Analysis. This mandates that banks assess various elements from banking sessions and adjust security protocols based on their findings. If a transaction deviates from historical patterns or there are signs of potential compromise, an alert should be activated, prompting further authentication steps. Conversely, the absence of irregularities allows for the omission of Strong Customer Authentication (SCA). Implementing and interpreting this process in real time can be complex.

While mandated in the EU, institutions in other jurisdictions can benefit from following the guidelines implemented by institutions that have been supporting real-time payments for nearly a decade.



ThreatMark's Behavioral Intelligence Platform

By implementing ThreatMark's Behavioral Intelligence Platform, financial institutions can enhance its ability to detect and respond to potential threats in real-time, especially crucial for real-time payments, and ensures compliance with PSD2 regulations. This proactive surveillance allows for a refined security posture that dynamically adapts to transaction risks while facilitating a smoother and safer banking

- **Reduced Fraud Costs**
  Expert tools and tactics directly combat phishing and malware, curtailing potential financial losses.
- **Operational Efficiency**
  Quick threat mitigation, due to relationships with key providers, minimizes disruptions and response times.
- **Enhanced Security ROI**
  Maximize the return on security investments by providing an all-encompassing defense.
- **Risk Management**
  Proactive threat hunting reduces unforeseen vulnerabilities, safeguarding the bank's assets and reputation.

MITIGATING SCAMS IN REAL TIME.

Strong & Invisible Authentication

Strong and invisible authentication crucially balances advanced security with a seamless customer experience. Utilizing technologies like behavioral biometrics and behavioral analytics, authenticating users subtly and effectively can minimize the risk of fraud and unauthorized access.

3D Secure Card Payment Authorization

Credit card transactions are a common target for fraudsters as they can easily obtain the cardholder's credit card data without being detected. To prevent this, 3DS introduces two-step authentication to every payment by default.

70%
Better detection rate
(than traditional FDS)

90%
Fewer false positives
(than traditional FDS)

90%
Decrease in cost for authentication
(ets. SMS cost saving)

2
Weeks to implement
(cloud option)

Improved detection & scoring methods
(when integrating with existing systems)

ThreatMark's Behavioral Intelligence Platform is the world's first full-stack fraud prevention platform built on behavior intelligence. Combining transaction risk analysis, threat detection, and user behavior profiling capabilities in one integrated platform, ThreatMark monitors signals including:

Instant Payment Risk Scoring

In vishing attacks, scammers use various tactics to avoid being caught including using high-priority transactions. Carefully examining the priority attribute of a payment is a method of preventing fraudulent transactions.

Active Phone Call

Scammers use coercion to manipulate victims acting against their best interest, often talking the victim through the money movement process. Monitoring for active phone calls during a banking session can be a signal of a scam in progress.

Abnormal Payment

Fraudulent payments can be identified by analyzing payment amount, time, day and month of transfer, and beneficiary. Examining payment context with other risk indicators can detect abnormal payments and disrupt fraud attacks.

Remote Access Tools (RAT) In Use

When scammers convince unsuspecting victims to install a RAT, they hijack legitimate banking sessions. The moment the scammer starts the tool, mouse movements, keystrokes, and other behavioral patterns indicate a RAT is in use.

Payment Tampering

Payment tampering fraud happens when someone intervenes with the payment process to divert funds, alter payment information, or manipulate transaction data. Discrepancies between payment details can reveal tampering.

Mobile Biometry Anomaly

Mobile behavioral biometry is used for continuous user verification. Observing each user's unique patterns of they how use a device during previous sessions, matches can be made in real-time to confirm if a user is legitmate.