ThreatMark

→ SUCCESS STORY



# HOW THREATMARK ENHANCED SECURITY & UX AND SAVED €1M A YEAR AT SLOVENSKÁ SPORITEĽŇA

*Slovenská sporiteľňa, part of Erste Group and one of Slovakia's largest banks with more than one million clients, wanted to strengthen security without adding friction for its customers. By partnering with ThreatMark, the bank replaced blanket SMS one-time passwords with AI-powered, risk-based authentication. The result: at least €1 million saved each year, dramatically less login friction, and full PSD2 compliance with sharper threat detection.*

## KEY CHALLENGES

Interceptable SMS one-time passwords, login friction for legitimate users, PSD2 compliance

## SMARTER AUTHENTICATION, LESS FRICTION

Like most banks, Slovenská sporiteľňa relied on SMS one-time passwords to authenticate customers at login. The approach was expensive, and caused major disruption for the majority of users who accessed their accounts for entirely legitimate reasons.

After consulting ThreatMark, the bank deployed ThreatMark Behavioral Intelligence, part of the ThreatMark Fraud Disruption Platform, across all of its digital channels. It continuously analyzes device data, behavioral biometrics, transactions, and contextual signals in real time, generating a risk score for every session. Low-risk logins proceed seamlessly, elevated-risk activity triggers step-up authentication, and high-risk attempts are blocked outright.

## STRONGER DETECTION, LOWER COSTS

During evaluation, the ThreatMark Platform identified 100% of cyber threats and delivered a 70% higher detection rate than competing solutions. With full contextual visibility into every session, the bank's fraud analysts also saw a 90% drop in false positives, freeing the team to focus on genuine threats rather than chasing noise.

The result is adaptive, risk-based authentication that meets PSD2 strong customer authentication requirements while keeping banking frictionless. Fewer than 10% of logins now require manual multi-factor authentication.

Cutting unnecessary SMS OTPs turned a recurring cost into measurable savings. According to the bank, ThreatMark's AI-powered authentication saves at least €1 million every year compared with previous SMS spend, while simultaneously improving the customer experience.

Customers feel the difference, too. Average time spent on the login page dropped by more than 50%, turning a routine security step into a near-invisible one. Security and convenience, long treated as a trade-off, now reinforce each other.

> *"The ThreatMark Platform was able to identify threats in 100% of test cases and showed a 70% better detection rate than other tested competitors."*

**JÁN ADAMOVSKÝ**
Chief Information Security Officer, Slovenská sporiteľňa

## KEY RESULTS

**70%**
Better Threat Detection Than Competitors

**€1M+**
Saved Annually by Reducing SMS OTPs

**50%**
Less Time Spent on Login Page

© ThreatMark 2026