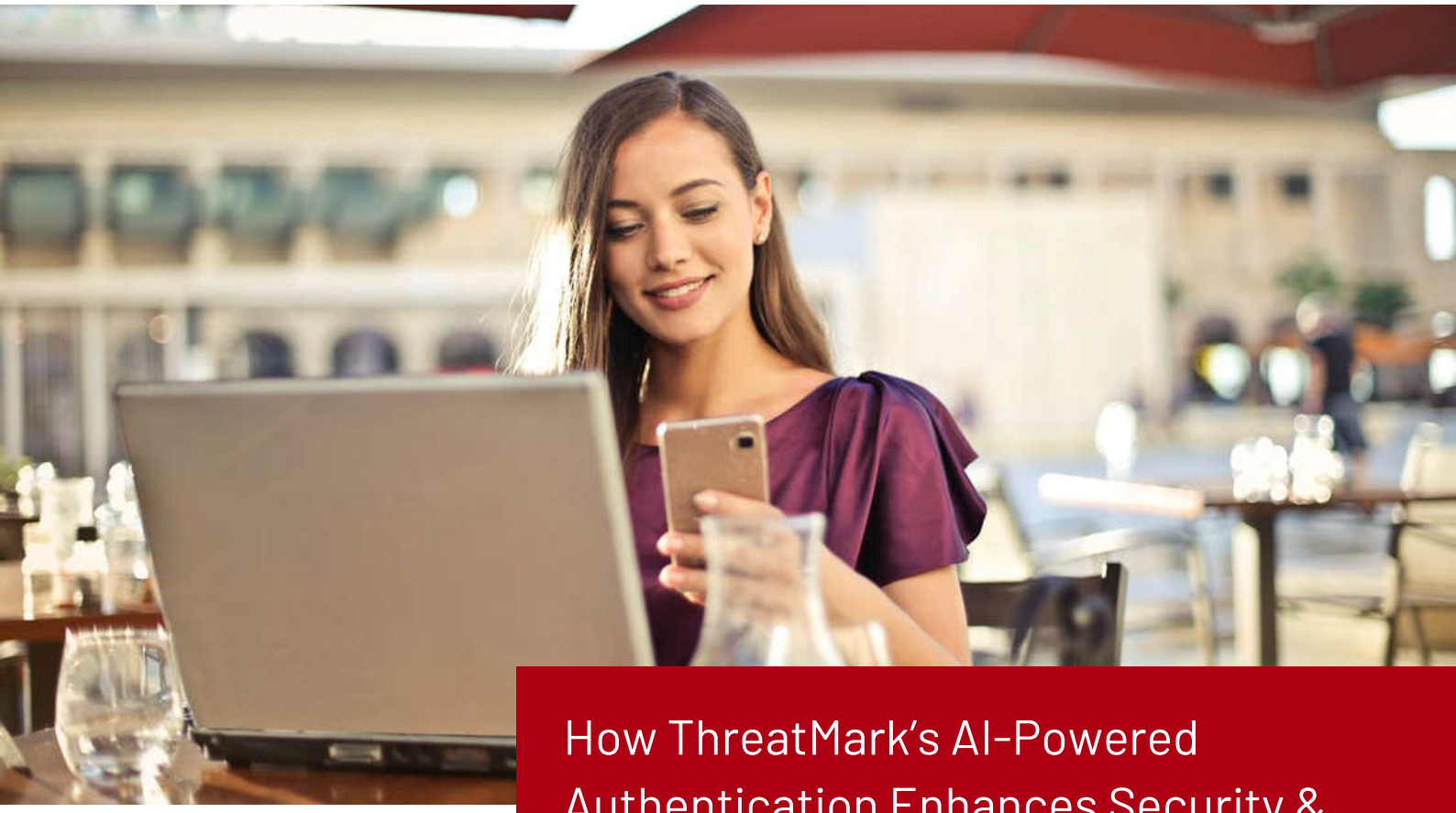
ThreatMark

SLOVENSKÁ sporiteľňa



How ThreatMark's AI-Powered Authentication Enhances Security & User Experience for Slovenská sporiteľňa (Erste Group)

SUCCESS STORY

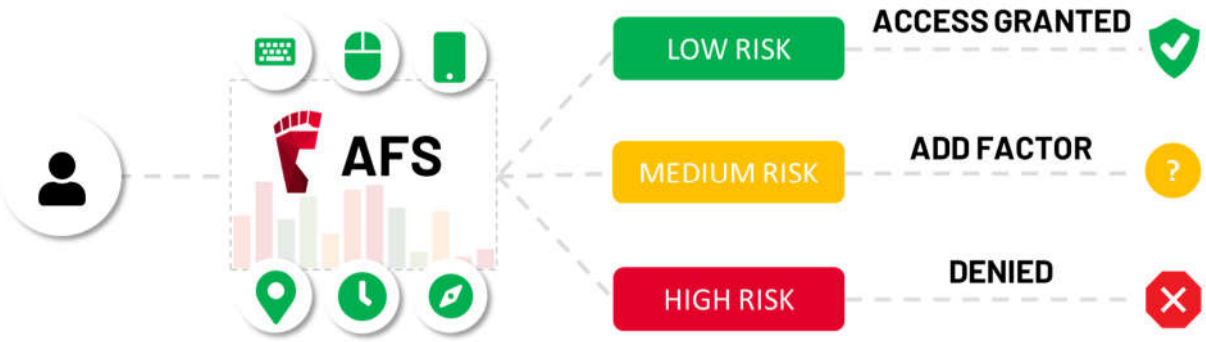
July 2020

Slovenská sporiteľňa, part of Erste Group, with over 1 million clients, decided to use ThreatMark's AI-powered risk-based authentication to upgrade its business flow & enhance security. As a direct result, the bank now saves at least €1 million every year while providing enhanced user experience for its clients. It is fully protected against various types of cyber threats & fully compliant with Payment Services Directive (PSD2) RTS requirements.

Slovenská sporiteľňa knew that the majority of users access their internet banking platform for legitimate reasons, and yet, they are bothered by one-time-password SMS's at every login. Many SMSs are sent in vain, and bank's end-users are unjustifiably **disrupted during their experience**. On top of that, sending SMS's is costly and it's **not secured**, as the messages can be intercepted.

After consulting ThreatMark, the Slovenská sporiteľňa has decided to deploy ThreatMark's Anti-Fraud Suite (AFS) for all their online channels. After a quick deployment, ThreatMark utilized **data about devices**, **user behavior** (behavioral biometrics), **transactions,** and other **contextual data across digital channels**. The collected data is

then processed in **real-time** using state-of-the-art machine learning algorithms and as a result a Risk Score is generated. If the Risk Score is low, the authentication element is not activated; when high, the authentication method (SMS) is escalated & sent.



With ThreatMark's adaptive user identification most users experience **frictionless authentication & seamless transaction authorization**. ThreatMark's system invokes strong authentication for high-risk logins and transactions only, meeting the necessary PSD2 requirements.

As a result, less than **10% of logins would require manual multi-factor authentication**, which **reduces friction dramatically**. High-risk logins or transactions are directly denied.

Per Ján Adamovský, the Bank's CISO, the ThreatMark's AI-Powered seamless-authentication did not only help with the PSD2 compliance but also **saved €1 million**, otherwise spent on SMS's (in comparison with previous years).

Previously, the bank's end-users usually spent **10 seconds on the login page on average**. With ThreatMark's AFS, this time has been **reduced by more than 50%**. Moreover, having the contextual info about each session and transaction ThreatMark identified **100% cyber threats during the test**.

ThreatMark showed a 70% better detection rate than the competition, preventing various types of cyber threats. The Bank's Fraud Analysts also noticed a 90% drop in false positives as a result of an in-depth overview of every session recorded in the AFS.

*„ThreatMark's solution was able to **identify threats in 100%** test cases and shown **70% better detection rate** than other tested competitors."*

Ján Adamovský, CISO

Our case study shows that Slovenská sporiteľňa, with 1M end-users, saves €1 million yearly & provides seamless user experience by implementing ThreatMark's AFS Solution.

Main Benefits Proofed by Slovenská sporiteľňa

The bank **Saves € 1 million yearly** by reduction of SMS OTPs

Detection capabilities of the bank were **improved by 70%**

Time spent on the login page dropped **by 50%** for end-users

Number of False-Positives **dropped by 90%**

ThreatMark's digital identity verification and fraud prevention solution is trusted by leading European banks protecting tens of millions of end-users and thousands of transactions every day.

ThreatMark s.r.o.

Hlinky 505/118,
603 00 Brno,
Czech Republic

IČ: 04222091, DIČ: CZ04222091

Contact us at:
info@threatmark.com