THREATMARK HELPS CSOB PREVENT 63% MORE FRAUD LOSSES

Faced with a surge in phishing and vishing attacks, Ceskoslovenska obchodni banka (CSOB) turned to ThreatMark's Behavioral Intelligence Platform to bolster its defenses. The results were immediate: the bank increased prevented fraud losses by 63%, improved its detection success rate by 29%, and significantly reduced the average loss per customer. With these successes, Ceskoslovenska obchodni banka plans to harness ThreatMark's fraud intelligence even further as it prepares for the upcoming PSD3 regulations.

KEY CHALLENGES

Phishing, vishing, scams

BACKGROUND

The rise in fraud at CSOB started to escalate in 2020, initially driven by phishing attacks. Fraudsters tricked clients into entering their login details on fake phishing sites, allowing them to access and drain victims' bank accounts.

By late 2020, vishing attacks emerged, further complicating the fraud prevention strategies in place. Fraudsters impersonated bankers, police officers, or IT support staff, manipulating customers into revealing sensitive information such as CVV codes. These tactics were often paired with remote access tools, allowing criminals to execute unauthorized transactions.

With fraud cases increasing in volume and sophistication, CSOB recognized the need for a more advanced fraud prevention solution capable of distinguishing legitimate transactions from fraudulent ones.

HOW DID CSOB OVERCOME THESE CHALLENGES?

After evaluating potential solutions, CSOB selected ThreatMark as its anti-fraud partner. The implementation of the ThreatMark Platform was seamless, supported by collaborative workshops between the bank and ThreatMark's team.

The impact was immediate. In 2022, before implementing the ThreatMark Platform, CSOB's fraud detection success rate was around 50%, leaving a significant gap in its defense strategy. By 2023, following integration, that rate dramatically improved, with 63% more fraud losses prevented, even as fraud cases tripled. In 2024, the ThreatMark Platform further enhanced detection accuracy and helped reduce the average financial loss per customer by 30%.

"We use the ThreatMark Platform to detect all types of fraudulent attacks, including fraudulent activations of our mobile authentication app and voicebot phishing, which would otherwise be difficult to catch," explains Lukas Eberl, FDS Product Owner. The bank's new practice of pairing devices via Bluetooth to transfer the authentication app has significantly reduced phishing incidents.

ThreatMark has also kept pace with increasingly sophisticated vishing. Initially, fraudsters used remote access tools, which the ThreatMark Platform detects by identifying RATs and screen-sharing activity, combined with behavioral intelligence. As tactics shifted toward social engineering, ThreatMark evolved too, detecting when customers were on the phone with scammers while using the banking app.

ADDITIONAL BENEFITS OF THE THREATMARK PARTNERSHIP

Beyond enhanced fraud detection, CSOB values the proactive and customer-centric approach of the ThreatMark team.

"Their responsiveness and ability to rapidly develop new detection capabilities based on emerging fraud trends is a significant advantage," notes Jakub Cerny, Online Fraud Analyst.

According to the bank, another benefit of the partnership is the participation in ThreatMark's Banking Fraud Summits, exclusive events where fraud specialists collaborate on strategies to combat emerging threats. The Summits provide an opportunity for industry professionals to exchange insights on the latest fraud trends, discuss best practises, and explore new detection methodologies.

"We see great value in the Summits. Demonstrating real detection scenarios on actual data would, in our view, further strengthen industry efforts in combating fraud," adds Jakub Cerny.

WHAT ARE THE BANKING FRAUD SUMMITS?

Banking Fraud Summits are exclusive events where banking professionals connect in a secure, sales-free environment to discuss emerging fraud trends, share real-world insights, and collaborate on effective prevention strategies.

> *"Improving detection scenarios is just one of the benefits of the ThreatMark Platform. By reducing false positives, we've been able to streamline our work. This is especially important as the number of attacked clients continues to grow, with an 11% increase during the first half of 2024."*

PREPARING FOR PSD3: FUTURE OUTLOOK

Looking ahead, CSOB remains committed to intensifying its efforts in the fight against fraud, especially in light of upcoming regulatory changes with PSD3. *"The shift in responsbility for fraud losses and the need to compensate defrauded clients will present a significant challenge. That's why we are currently testing the transaction monitoring module of the ThreatMark Platform. Reliable fraud detection and robust data analytics will be crucial in preventing financial and reputational damage,"* explains Lukas Eberl on behalf of fraud prevention team at CSOB.

Educational initiatives to raise fraud awareness among clients are another integral part of the bank's strategy, as customers play a key role in the fight against fraud.

"Even with the best fraud detection tools, customer awareness is essential, as some clients still proceed with transactions despite clear warnings. Ultimately, our role is to detect fraudulent activity without hindering legitimate banking operations—ThreatMark is instrumental in achieving this balance," concludes Lukas Eberl.

KEY RESULTS

63%
Increase in prevented fraud losses

29%
Increase in detection success rate

↘
Reduction in false positives

LEARN MORE ABOUT THE THREATMARK PLATFORM