

HOW CPN ECUADOR ERADICATED NEW ACCOUNT FRAUD WITH THREATMARK

Cooperativa de la Policía Nacional (CPN) is a leading financial institution founded in 1976 to serve Ecuador's National Police and their families. Now open to the public, CPN provides tailored financial services—including savings, loans, and investments—to nearly 200,000 members. With a strong focus on security and trust, the cooperative has reinforced its reputation as a safe and reliable institution by implementing ThreatMark Behavioral Intelligence, significantly enhancing customer protection and reducing financial losses.

KEY CHALLENGES

New account fraud, reputation risk, and customer friction

The challenge of new account fraud was compounded by the need to maintain trust and satisfaction among CPN's unique customer base, consisting largely of Ecuadorian police officers and their families. This clientele relies heavily on CPN for critical financial services and expects a seamless, secure banking experience that matches their distinct needs. With minimal tolerance for delays or disruptions, CPN needed a solution capable of preventing fraud in real time without introducing unnecessary friction. In a sector where both security and user experience are paramount, CPN recognized that balancing effective fraud prevention with high customer expectations was not merely beneficial—it was essential.

Driven by the pressing need to safeguard its reputation and provide uninterrupted services, CPN embarked on a search for an adaptive and automated fraud prevention solution.

WHAT PROMPTED CPN TO RETHINK FRAUD PREVENTION

Before implementing ThreatMark, CPN faced significant challenges in preventing fraud, with new account fraud posing the most serious threat. Fraudsters exploited CPN's loan services by creating accounts, obtaining quick loans, and rapidly transferring funds out of the bank. This resulted in significant financial losses within the first half of 2020.

With security processes relying on manual, parameter-based methods, CPN found it increasingly difficult to keep up with the sophisticated tactics fraudsters were using, allowing multiple instances of fraudulent account openings to go undetected. This considerable financial burden underscored the urgency for a solution that could halt losses swiftly and accurately.



"Since *implementing the ThreatMark Platform, we haven't lost a single dollar to fraud. The difference has been remarkable. We went from facing hundreds of thousands in losses to complete security, giving both our team and our clients confidence that their money is safe with us.*"

ANDRES ESPINOSA
Information Security Architect

© ThreatMark 2025

HOW DID CPN OVERCOME THESE CHALLENGES?

After a thorough evaluation of available technologies, CPN Ecuador selected ThreatMark Behavioral Intelligence, part of the ThreatMark Fraud Disruption Platform, for its adaptability, responsiveness, and proven performance during testing. "*I investigated a lot*," said Andres Espinosa, Information Security Architect at CPN, noting how the platform was the clear choice for addressing the cooperative's specific fraud challenges. Its ability to be tailored to CPN's environment ensured a strong fit from day one.

With implementation of the ThreatMark Platform, CPN moved from manual controls to fully automated, real-time fraud detection. Continuous behavioral user profiling in Behavioral Intelligence – Identity enabled instant identification of suspicious activity, stopping fraudulent transactions before any financial impact could occur.

"*Since implementing the ThreatMark Platform, we haven't lost a single dollar to fraud*," Andres shared. "*The difference has been remarkable. We went from facing hundreds of thousands in losses to complete security, giving both our team and our clients confidence that their money is safe with us.*"

Within just one week, the ThreatMark Platform had also reduced false positives—allowing members to continue banking smoothly and securely. "There is no friction for our customers," Andres added, highlighting how the platform provides strong protection without disrupting the member experience.

Beyond fraud prevention, the partnership brought lasting organizational benefits. CPN Ecuador reinforced its reputation as a trusted institution—especially important for a cooperative serving the law enforcement community. Member satisfaction increased as the fraud-free experience deepened confidence in CPN's services.

"*With CPN, I know my money is safe*," Andres emphasized. This sentiment, shared across the member base, has become a reflection of the cooperative's strengthened security posture.

Operationally, the platform's automation reduced manual workloads and freed up the security team to focus on strategic, proactive initiatives. This shift created space for professional growth and innovation within the bank.

The financial savings from stopping fraud have been reinvested into digital banking improvements, further enhancing the member experience. Additionally, the ThreatMark Platform has played a critical role in CPN's compliance readiness—helping the institution meet evolving regulatory requirements efficiently and reinforcing its position as a forward-thinking, member-first organization.

STAYING AHEAD OF REGULATION AND RISK

As Ecuador moves toward alignment with European data protection standards and evolving financial regulations, CPN Ecuador is well-prepared. The flexibility of the ThreatMark Platform ensures CPN can continue to meet complex compliance requirements, including advanced data protection and fraud prevention mandates.

This adaptability allows CPN to maintain a leadership position in a more tightly regulated environment—without compromising service quality or member trust.

Looking ahead, the ThreatMark Platform will remain central to CPN's strategy. As the cooperative expands its digital offerings and strengthens its defenses, the platform provides the resilience needed to stay ahead of emerging threats and deliver continued security for its 200,000 members.

KEY RESULTS



100% elimination of new account fraud



Reduction in false positives



Decreased manual workload



Improved customer experience

LEARN MORE ABOUT THREATMARK BEHAVIORAL INTELLIGENCE

© ThreatMark 2025