



SAFE PAYMENT ECOSYSTEMS

The ability to fight fraud in payments has come a long way since the days of analog fraud detection. At that time, for every transaction, a cashier would comb through a thick book of stolen cardholder account numbers or dial up a call center representative to authorize a transaction.

We can track the development alongside the evolving World Wide Web. To begin with, the cards used only the magnetic stripe. With more interactive internet, the chip-and-pin and contactless payments have been developed, followed by tokenization and enhanced data sets that approve transactions.

AI IN THE SERVICE OF CYBERSECURITY

Throughout this dynamic development, artificial intelligence has played a key role in ensuring the security of payments. Visa pioneered the use of AI models in this area in 1993, becoming the first payments network to use neural network-based technologies for real-time, risk-based fraud.

"Cybersecurity is at the heart of everything we do. Our focus is to reduce the risk throughout the payments ecosystem and AI has been a proven tool to do so," says Ľubica Gubová, Country Manager Visa Slovakia.

Visa is currently using more than 60 AI models to ensure safer and smarter movement of money and to prevent fraud before it happens. Over the last five years, we have invested roughly 500 million US dollars in AI and data infrastructure. The company can draw on data from 4.2 billion card accounts and transactions worth 13 trillion euro to catch unauthorized transactions efficiently.

In 2022 alone, Visa's real-time payment fraud monitoring solution, Visa Advanced Authorization (VAA), helped prevent an estimated 27 billion US dollars in fraud by deploying advanced predictive models. Soon, Visa's deep learning models will help break through an industry authorization conundrum – reducing fraud while improving the approval rates essential to minimizing

consumer frustration over false declines.



Cybersecurity is at the heart of everything we do. Our focus is to reduce the risk throughout the payments ecosystem and AI has been a proven tool to do so.

ĽUBICA GUBOVÁ



SEAMLESS TRANSACTIONS MILLION TIMES A DAY

Visa's uncompromising commitment to security has kept fraud at historic lows: less than 0.1% of

The technology behind how people shop is constantly changing and improving. Customers expect to pay conveniently, easily, and securely at all times. The shift to digital money is incredibly exciting but it also places exponentially greater pressure to ensure every transaction is secure and reliable. Visa has been using artificial intelligence to prevent fraud and to provide security in payments already for 30 years.

transactions – among the lowest of all payment forms. In Slovakia, the share of fraud in all card transactions is even half lower compared to the European average and has been decreasing.

"Our infrastructure is exposed to an average of 2 million cyber threats every day. We protect tens of thousands of transactions every single second, all over the world," Ľubica Gubová explains.

However, as payments technology and authentication have become more secure, fraudsters are now targeting consumers directly. It is thus important that consumers know how to protect themselves.

THE NEW AGE OF AI

Thirty years after launching the use of AI models in payments, Visa considers three areas as critical to the next decade of AI innovation – extending its expertise in fraud detection and security; establishing exceptional levels of resilience for partners across its network; and commitment to the

highest standards of data governance.

Service downtime from an unexpected outage or scheduled maintenance is disruptive for financial institutions and their customers. To meet the need for resilience and security during these times, Visa has developed tools powered by AI and machine learning to help in situations like improving payment experiences during bank outages.

It is a collective responsibility to make sure AI is used responsibly and ethically. Visa has created a governance structure that prioritizes ethics to help ensure the responsible stewardship of five core data values: security, control, fairness, accountability, and value.

"Fraud prevention and security will always be the fundamental focus for Visa. However, we see the ethical governance of data and our ability to enable previously out of reach levels of uptime as core to the next 10 years of our AI product development," adds Ľubica Gubová in conclusion.

HOW TO SHOP SAFELY

- Always check the URL when shopping online. The letter "s" in the word "https" means that it is secured.
- In a store, use a payment card with a chip or contactless payment symbol, or a mobile wallet.
- Beware of phishing. Keep your personal information to yourself. Do not click on links before you verify that they will take you where they say.
- Software updates are essential. Always install the latest software updates on your computer, tablet, or phone before shopping.
- Avoid public Wi-Fi: Do not shop online over public Wi-Fi networks. Use a secure password-protected network or mobile data connection when shopping online.

CYBERSECURITY SLOVAKIA VS. EUROPE

- In Slovakia, the share of fraud in all card transactions is half lower than the European average in terms of the volume of Visa transactions.
- The ratio of fraudulent transactions has been decreasing in the last 12 months.
- Technological maturity of Slovakia in the field of digital payments is high. We are among the first in Europe to introduce modern technologies.
- There is a high proportion of mobile payments in Slovakia – tokenized payments provide maximum security.