

*Instant,
reliable, trusted
fraud prevention.*

Case Study: QIWI

IRIS Analytics helps QIWI defend its reputation

The Scope

Company

A leading provider of next generation payment services in Russia and the CIS

Channels

Self-service kiosks (pay in), e-wallets, Visa prepaid cards (virtual and plastic)

Territories/markets

Russia

Customer numbers

70 million consumers, 167,000 kiosks, 15.5 million e-wallet accounts

Transaction values

RUB 49 billion cash and electronic payments per month

Time to implementation

A complete solution to protect QIWI customers against fraud implemented in only five weeks

The Challenge



- QIWI wanted to defend and improve its reputation in the market as a reliable and trust-worthy payment platform.
- It wanted to respond quickly and effectively to future threats which they did not necessarily know about or could not define/anticipate in advance.
- QIWI believed that increased future regulation of the payments industry in Russia would make fraud prevention and risk management systems like IRIS a “must have” requirement.

“IRIS provides us with the confidence that we can immunise our services against any type of fraud patterns within a matter of hours. This is good news in terms of our expansion, not only in Russia, but also into new markets.”

Anton Kuranda, Chief Security Officer, QIWI Group

The Solution

IRIS Analytics installed IRIS 5, its award-winning real-time fraud and risk control solution in QIWI's existing virtual-server based IT environment.

IRIS profiles all monetary and non-monetary transactions over each of QIWI's lines of business in real-time.

The Implementation

QIWI needed a solution very quickly. The QIWI IT landscape of virtual-servers running Linux was ideal for IRIS, and an implementation project was kicked-off. IRIS is an "off-the-shelf" package, and as standard integration into the IRIS solution utilises the most modern industry standards available, and a fully integrated system was delivered in just five weeks.

The Results

- QIWI is able to not just defend, but to enhance their reputation as a reliable and trustworthy payment platform in the Russian market.
- QIWI is able to respond to new threats in a matter of just hours.
- Today QIWI owns the most advanced payment platform in the Russian market for fraud prevention and risk control. Future regulation, if it comes, will not be a challenge for the QIWI platform and neither would future, as yet unknown threats.

Interview



Anton Kuranda

Chief Security Officer,
QIWI Group

What were QIWI's challenges before choosing the IRIS fraud prevention solution?

Our challenges are not only about reducing fraud losses, but also keeping our services open to customers in the event of a massive fraud attack. Because our services are optimized to be versatile and convenient for our customers, we are a frequent target of criminal attacks. Some of these attacks are rather innovative and we cannot anticipate them in advance. A recent large-scale attack with fake bank notes is a clear example.

What has impressed you most about the solution?

From the first day of using IRIS we were able to stop the fraud patterns that we had seen before. Over the next weeks our fraud experts began to adapt the initial decision models created by IRIS Analytics specialists on their own, and became fluent in devising countermeasures against many other types of fraud as soon as such fraud patterns emerged.

The Benefits

- IRIS is designed as a multi-channel fraud prevention system, and can create any number of data streams with any types of variables in IRIS with the click of a mouse.
- It can define rules and procedures on how these data streams should be combined to perform behaviour profiling, also without any line of code.
- The same IRIS installation can therefore protect traditional payment channels such as credit and debit cards from the issuer and acquirer side, as well as e-commerce, online banking, and e-wallet channels.