



NetGuardians

# CASE STUDY

ZÜRICH

KANTONALBANK

SWITZERLAND



Zürcher  
Kantonalbank

The Swiss bank had only a narrow window in which to install a fraud-prevention solution that would detect behavior anomalies associated with a payment without generating excessive false alerts. Here's why it chose NetGuardians.




Our main requirements were to detect more fraud with a flexible system that would throw up fewer false positives. We were getting about 800 false alerts a day. With NetGuardians we have cut that and are stopping more fraud.

**Romano Ramanti**  
**Ethical Hacker**  
**Zurich Kantonalbank**



# The Requirement

Zurich Kantonalbank (ZKB) is the biggest of the Swiss cantonal banks and the fourth largest bank in Switzerland. It is a universal bank, offering a full range of services including international. Established in 1870, today it has assets of some CHF192 billion, operates more than 50 branches and has a strong regional focus on the canton of Zurich.



The bank wanted to spot more fraud, particularly new and emerging fraud types where the fraudster poses as the account holder. It also wanted to cut the number of false alerts from about 800 a day.

Finally, the bank wanted a flexible tool that would allow it to set new rules within the vendor's own ecosystem rather than on ZKB's Java-based, self-built core banking platform.



## The Solution

When Romano Ramanti, ethical hacker at Zurich Kantonalbank, was charged with coming up with a proof of concept for a new fraud-prevention system in 2019, he remembered NetGuardians from a talk he had attended a couple of years earlier. At this event, Joël Winteregg, NetGuardians' co-founder and chief executive, had described new banking fraud-prevention software that focused on behavior, using artificial intelligence and machine learning to build highly detailed customer profiles. The software compared all transactions against the profile, raising an alert when something was out of character.

Mr. Ramanti invited NetGuardians and one other provider to develop proofs of concept; NetGuardians won.

The project was not straightforward. One of the biggest problems was finding the right data.

” We knew we had it all, just not necessarily where it was located, says Mr. Ramanti.

Another challenge was to link the NetGuardians platform with that of the bank.


NetGuardians software is a plug-and-play solution compatible with the world's largest core banking platform providers. Given ZKB's platform was self-built, it meant building bespoke messaging systems to carry payment data between it and NetGuardians. All transactions are first processed by the bank, then sent to NetGuardians for screening.

Implementation began in April 2021 with the bank adopting NetGuardians' AI risk models. Initially, ZKB believed it had up to six months to complete the project, but very quickly that window was reduced to three.

” The revised timescale was challenging, but we managed it, mainly thanks to NetGuardians, Mr. Ramanti says.

Besides setting up the AI risk models, NetGuardians also helped ZKB find new fraud types. These included model adaptations to detect a common Microsoft support scam, where the criminals claim to be calling from the U.S. software giant. Under this scam, the payments go through a Revolut account; this IBAN number was built into the models. “If you need to, NetGuardians gives you the ability to write rules to suit your own bank, but these rules aren't held on your core banking software. It's much more flexible. It's great. We love it,” he says.

ZKB went live with NetGuardians in June 2021.



” The shortened timescale meant we had to delay some functionality. We split it up between what we really needed and what would be nice to have. Everything we needed got done for launch, Mr. Ramanti says.

This meant ZKB had a fraud-prevention solution that could spot frauds where behavior was out of character, even when there was no technical anomaly.

If a customer’s usual range of payments is between CHF100 and CHF10,000, when a fraudster takes over a laptop and makes a CHF40,000 , that’s the kind of fraud we were able to spot with NetGuardians, he says.

Some of the delayed functionality included streamlining processes such as releasing payments.

” We realized this could be fixed at the second stage without affecting reliability, he says.

# The results

” We’re stopping more fraud cases a month. It’s working really well, says Mr. Ramanti.

The bank has two full-time employees who monitor the fraud alerts.

” We still get up to 700 false alerts [down from 800 a day under the old system], but we are screening more transactions and stopping more fraud. Our first goal was to significantly improve fraud detection. The focus on the reduction of false alerts was secondary but still critical. It’s great that we can spot and stop more fraud while still reducing the false alerts. Thanks to the explainable AI, there’s more contextual information for our team to work with and they can work better as a result, he says.

Just over a year after full implementation, Mr. Ramanti is keen to extend the relationship with NetGuardians. “There are more AI risk models that I’d like to implement to cover emerging threats. We’re looking at using behavior analytics to detect typing speed, for example,” he says. “I’m sure there will be other areas too.”



# Contact us

## NetGuardians Headquarters

Y-Parc – Avenue des Sciences 13  
1400 Yverdon-les-Bains  
Switzerland  
+41 24 425 97 60

## NetGuardians Africa

The Mirage Tower 1, 12th Floor  
P.O. Box 574  
00606 Sarit, Nairobi  
+254 796 616 263

## NetGuardians Asia

WeWork | NetGuardians  
71, Robinson Rd, #14-01  
Singapore 068895  
+65 6224 0987

## NetGuardians Eastern Europe

WeWork  
Krucza 50, 00-025  
Warsaw, Poland





**NetGuardians**