Case Study

BforBank

How an Online Bank Exposes Complex Fraud with Graph Database Technology

INDUSTRY
Financial Services

USE CASE
Fraud Detection & Analytics

GOAL
- Reduce time spent querying information across siloed systems and detect sophisticated fraud schemes

CHALLENGE
- Complex fraud rings and tactics often go unnoticed because deception relies on layers of indirection

SOLUTION
- Visualize connections within the data, uncovering hidden relationships and complex fraud ring schemes

RESULTS
- Faster investigations via shorter response times, with 20% more fraud attempts prevented
- Detection of several dozens of fraud cases unveiling complex fraud rings

French online bank BforBank needed to be able to detect and act on fraud more quickly and efficiently. They turned to Neo4j graph technology and Linkurious Enterprise to reveal previously hidden connections across multiple data silos and uncover complex fraud.

The Company

BforBank is an online bank launched in 2009 by Crédit Agricole Group. With more than 180,000 customers, the bank is one of the leading financial institutions in the French online banking market, providing services such as checking, debit and security accounts, life insurances, home loans and consumer credits.

Our Partner

Linkurious is a long-time Neo4j solution partner based in Paris, France. The company helps government agencies and Global 2000 companies detect and investigate sophisticated threats faster. More than 60 organizations worldwide use the Graph Intelligence Platform Linkurious Enterprise.

This distributed web application allows non-technical users to search, visualize and edit data stored in Neo4j. Investigation teams can collaborate to leverage rich visualizations of data and graph analysis features to expose connections, reveal patterns of interest and find insights hidden in complex connected data.

The Challenge

BforBank faced a real challenge identifying complex fraud schemes in siloed data. Every day, BforBank's database management systems collect large amounts of data. From transactions and money flows to Know Your Customer (KYC) documents, the bank has large volumes of structured and unstructured data distributed across multiple silos. Monitoring this data is critical to lowering risks and financial losses.

To investigate flagged customers, transactions or behaviors, the bank's risk and compliance team was using a bank fraud solution built on relational technology. As a result, querying connections within the data to confirm fraudulent activities or uncover fraud rings was a tedious, long and sometimes unsuccessful process.

"A request could take from two minutes to several hours when querying for connections across multiple relational tables. Cross-field queries could take several days," said Alexandre Dressayre, Compliance Officer at BforBank.

Complex cases required access to information scattered across data silos. Some types of fraud, such as phishing, required the intervention of the IT Department.

Case Study

"The processing time to identify fraud rings was divided by 10. In a recent investigation, a ring of 11 fraudsters was detected and identified within half an hour."

– Alexandre Dressayre, Compliance Officer BforBank

Every time investigators had to request additional technical resources, this slowed down the fraud investigation process, potentially resulting in larger losses. The bank needed a more effective way of monitoring all its data to reduce risk and financial losses.

The Solution

To improve fraud detection and reduce investigation time, BforBank looked to graph database technology. Linkurious provided a bundled solution with Linkurious Enterprise software, which offered off-the-shelf visualization and analysis on top of Neo4j's graph database. According to Dressayre, it was the perfect fit.

BforBank's risk and compliance team started by designing a data model, loading all customer data, bank transfer orders, check cashing activities and IP addresses into Neo4j. The graph data was instantly available, providing an intuitive interface to investigate the hidden connections of suspicious clients.

"Thanks to the available network of data, we can spread out the connections and try to find if a fraudster is connected to other clients, through IP, postal or email addresses, for example. This helps us detect fraud rings or identity theft fraud," said Dressayre.

Now the BforBank team is able to detect fraud patterns that were too complex to identify in the past.

"The first pattern we set up was one related to phishing fraud. The system reports cases where clients have multiple and suspicious connection behaviors," said Dressayre.

And, as new fraud schemes are identified, BforBank can set up additional alerts to oppose those threats.

The Results

The risk and compliance team can now easily query connections and specific patterns within the data – as a result revealing complex fraud scenarios that had remained undetected in the past. Since implementing graph database technology, BforBank has reported an **increase of 20% in fraud attempts stopped in their tracks**.

The bank has also seen a huge reduction in the time needed to complete investigations, leading to quicker decisions and faster regulatory reporting.

"The processing time to identify fraud rings was divided by 10," said Dressayre. "In a recent investigation, a ring of 11 fraudsters was detected and identified within half an hour." Previously, before the implementation of Linkurious and Neo4j, a similar complex case would have taken several days to complete.

With a clear view of all its data connections, the risk and compliance team is now able to uncover and act on fraud much more quickly and efficiently, preserving the financial integrity and the reputation of the bank.