09 — 19

Simulation For Fraud Analytics

Next Generation Tools

Simudyne — Reality, re-engineered

PART I

Simulation for Fraud Analytics

Reports indicate that the global cost of financial crime has topped $3 trillion, with consumers losing nearly $1.5bn to fraud last year. Criminals are targeting institutions due to their permeable controls and no one wants to be the weakest link.

Luckily, the next generation of fraud analytics tools will make your detection process easier, quicker and cheaper – and significantly minimise false positives – allowing you to prepare for both current and future threats.

Why is this needed?

An industry-wide challenge for fraud detection is the lack of objective data-driven testing and evaluation of current transaction monitoring systems.

Historical data is not enough

Current approaches to fraud analytics, such as false alarms optimisation, are limited to classic techniques that use historical data to analyse and improve their performance, meaning that progression is limited to observations in the past.

Complexity of modelling real world environments

Simulating financial transactions is a real challenge. A model's ability to reproduce realistic behaviours is dependent on quality calibration of data.

Unexpected fraud behaviours and rare events

Fraud data is inherently imbalanced and hard to model. The most common method used today to prevent illegal transactions consists of tagging clients according to perceived risk and restricting their transaction activity. Given the static nature of these controls, they fail to detect the adaptive behaviour of criminals.

Data privacy issues

It's difficult to procure and get approval to use real transaction data due to privacy laws like GDPR.

This is the case even for banks trying to use their own customer data.

The problem with false positives and hidden fraud

Current control methods focus only on two things to measure the improvement:

- Reducing the number of innocent people wrongly tagged (False Positives)
- Increasing the number of criminals flagged (True Positives)

Yet current detection systems do not consider the False Negatives (un-detected criminals), because this information is unknown.

With the aid of advanced fraud analytics tools such as simulation, we are now able to generate information about the missing crime (False Negatives) and calculate the reduction of fraud. This significantly changes the way we do things now and gives us a new horizon to improve current control systems.

> “ Despite all of the money we’re spending — and we’re spending a lot of money to keep criminal money out of our institutions — it’s still getting in every single day, right by all those controls.”

JENNIFER CALVERY
GLOBAL HEAD OF FINANCIAL CRIME THREAT MITIGATION AND GROUP GENERAL MANAGER, HSBC.

PART II

Simulation as a Support Tool

Simulation has proven to be indispensable to tackling several real-world challenges for detecting and preventing financial crime. By simulating millions of potential scenarios, you can create synthetic data that is essential to identifying the level of fraudulent activity that isn't being picked up by current systems.

Synthetic data

What's so powerful about agent-based simulation is that it uses real data to calibrate the required parameters that allow the creation of realistic synthetic datasets. After the enforcement of GDPR in late May 2018, many organisations are interested in methods that either comply with or avoid handling personal information. Fraud simulation is a novel and valid approach which involves the use of simulators to produce synthetic data.

Synthetic data contains no personal information or disclosure of legal or private customer transactions, so it is completely compliant with privacy regulations like GDPR. It has the added benefit of being easier to acquire, faster and at less cost for experimentation, even for those that have access to their own data.

Simulating a bank payment system

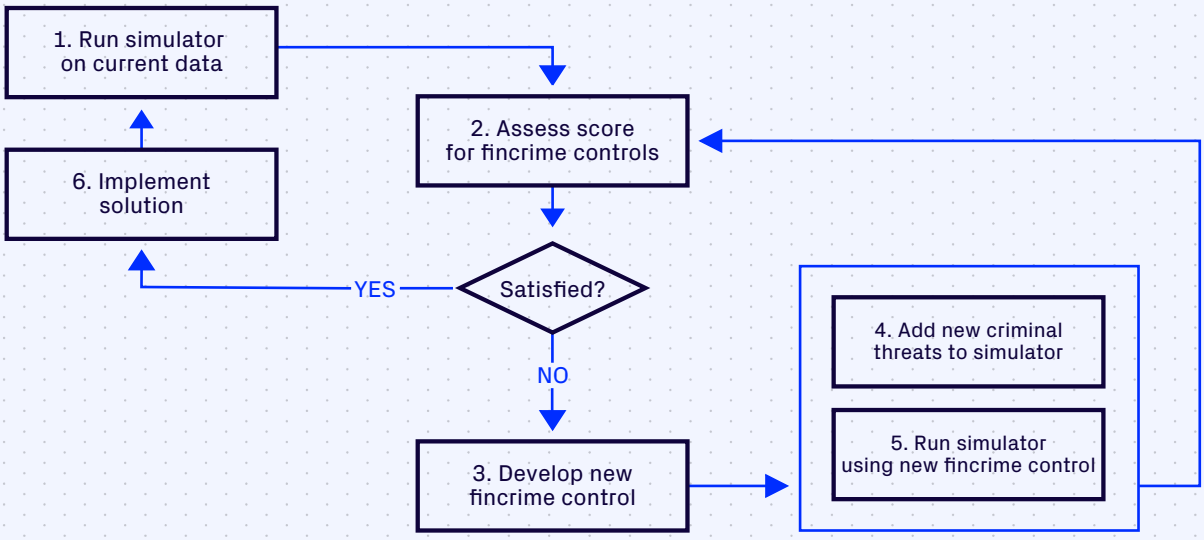
Organisations can produce a simulation that resembles a bank payment system, using synthetic data based on real customer transactions. Within the simulation a bank might recreate three agents: merchants, customers and fraudsters, all of which interact with each other.

For example, a customer agent might decide to purchase an item from a merchant agent. If accepted, the transaction takes place and the payment is registered. At the same time, their criminal counterparts move around the simulated environment and steal customer data in order to fraudulently purchase goods or services. Crucially, this generates labelled examples of fraud over time, some of which might have not yet been identified from current, real world datasets.

Self-evaluate your fincrime controls

Improving fraud detection is an ever-evolving process. Organisations are empowered by simulation to:

- Continue the development of the simulation model and extend the coverage of criminal cases.
- Incorporate simulation as part of their process for improving detection methods.
- Carry out exploratory analysis of foreseen or upcoming scenarios and evaluate current or newly developed controls.
- Continuously calibrate the simulator based on business data to measure the quality of fraud controls.
- Prove not only compliance with the law but also engagement in a proactive analytics programme inside the bank.



PART III

Key Business Benefits

Simulation is the bedrock of AI and Machine Learning. Only by harnessing the power of simulation and the next generation of fincrime analytics tools can banks improve their detection processes and prove to regulators that they have the appropriate controls in place.

What does this mean for your business?

- Advanced capability to train and test advanced control systems
- Flexibility to tailor scenarios of simulated financial crime to adapt to changing behaviour and environments
- Scalability to add increasingly complex scenarios of criminal behaviour and suspicious activity
- Provision of realistic synthetic data to avoid data privacy issues
- The security of running on premise without data leaving the organisation

Explore diverse scenarios and be prepared for them

For the first time algos can be optimised to run in environments that rarely occur, such as in rare fraud cases or events such as Brexit. Generating synthetic data would also be helpful where there is a significant change to either the customer's internal policies or regulatory rules.

Create training datasets with no historical precedent

Unlike statistic-driven models that are tied to past data, agent-based simulations are capable of using historical data to produce new, unseen and less imbalanced fraud training datasets that reflect the possible behaviour of future events. Criminal behaviour would try to adapt to side-step these changes and the original historical data would be less helpful for training new classifiers.

Agent-based simulation is quick and cost-effective

The nature of agent-based simulation is that agents do not need to run consecutively and can be distributed across machines to run concurrently, speeding the process up by many multiples.

PART IV

Why Simudyne

Simudyne is the market leader in agent-based financial simulation supporting advanced fincrime analytics. A partnership with Simudyne ensures you have the industry's most advanced financial crime simulation technology with support from the leading experts in the field.

Our software provides a robust library of code and examples for frequently used and specialized functions that saves time and reduces the complexity of detecting financial crime in an evolving environment. What normally requires several months of engineering and thousands of lines of code can now be delivered at a fraction of the time and cost.

Simudyne uses the firm's existing infrastructure to ensure it is cost effective and easy to deploy. As a deployed solution, the technology is safe and secure. It sits behind the customer's firewall and all the bank's data and models remain proprietary.

Our solution

- A base model to develop an advanced capability in training and testing financial crime control systems.
- Flexibility to tailor scenarios of simulated crime to adapt to changing behaviour and environments.
- Scalability to add increasingly complex scenarios of criminal behaviour and suspicious activity.
- Provision of realistic synthetic data that avoids data privacy issues.
- A more complete understanding of the dynamics of their customer transaction network.
- A sharable resource to comply with privacy regulations.
- The security of running on-premise without data leaving the organisation.

A: St Michael's Alley, London, EC3V 9DS

E: info@simudyne.com

W: simudyne.com

TW: twitter.com/simudyne

LI: linkedin.com/company/simudyne

Simudyne is a rapidly growing technology business, harnessing the power of advanced simulation, to help organisations make radically better decisions. Our efficient and scalable simulation platform allows enterprises to create a virtual environment where they can test drive their decisions, fail fast without consequences and create solutions that drive growth.

Sources:

https://www.bloomberg.com/news/articles/2019-04-04/global banks-beef-up-money-laundering-controls-as-fines-sting

https://www.accountancydaily.co/global-cost-fraud-tops-ps3-trillion

https://www.cbsnews.com/news/fraud-takes-over-as-consumers-top-complaint-to-ftc/