09 — 19

Uncovering Hidden Financial Crime Through Advanced Simulation

A Bluepaper from Simudyne

Abstract

Banks have invested, and continue to invest, billions of dollars to stop financial crime.

Yet with the global cost of fraud rising every year it is clear that we are failing to win the battle. In this bluepaper, we look at the inherent problem with developing better controls in the financial crime domain and explore how institutions can make significant improvements using simulation.

Instead of looking backwards at historical data, simulation can be used to train detection agents, test current methods and better prepare for future threats.

1.0

Introduction

Reports indicate that the global cost of financial crime has topped $3 trillion,[1] with consumers losing nearly $1.5bn to fraud last year.[2] In fact, we estimate that as many as 4 in 10 card transactions are now fraudulent, rising in some cases to 6 in 10.[3]

Digitisation has a large part to play in the growing levels of financial crime. As economies continue to move from analogue to digital, they become more accessible and often more vulnerable to breaches.

Combating money laundering is an enormous task and comes with substantial costs and risks. Meanwhile, criminals are getting ever more sophisticated at targeting permeable controls and continue to move illicit funds through the system to supply terrorism, drug trafficking and human trafficking. In response, regulators are increasing collaboration with other national agencies and are expecting better information and industry led initiatives from financial firms.[4]

Clearly, it is crucial for organisations, industry bodies and regulators to continue to improve their financial transaction monitoring systems to combat this threat against society. Banks are starting to take the right steps, looking towards Machine Learning (ML) and Artificial Intelligence (AI) to transform back office operations.

However, privacy laws like GDPR make it difficult to get approval to use real transaction data – posing significant challenges to ML and AI initiatives.

It is obvious that there is an inherent problem of developing better controls in the financial crime domain. In this whitepaper, we look at the reason detection systems are failing, and why simulation holds the key to winning the battle against financial crime. For wider academic reading on the topic, please refer to page 14 of this document.

> “ The FCA are placing an emphasis on collaboration and innovation to tackle financial crime. The increasing convergence of financial crime risks and improved cross- industry collaboration could lead to a significant change for the future of financial crime risk management”
>
> DEBBIE WARD, EY FINANCIAL CRIME[4]

2.0

Why aren't we winning the battle?

Banks have invested, and continue to invest, a significant sum of money to stop financial crime. It is estimated that Anti-Money Laundering compliance costs more than US$25 billion in the United States alone.[5] So, why aren't we winning the battle?

> "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[9]

Rules-based transaction monitoring

Banks have spent billions on transaction monitoring systems that scrub their accounts for possible money laundering schemes. Detection rules are action-based and target suspicious transaction behaviors, such as excessive cash deposits, structured transactions intended to avoid government record-keeping thresholds, and rapid money movement through one bank to another.[7]

However, this method significantly increases the number of false positives; it is estimated that only 1 in 5 transactions declared as fraud are truly fraudulent, and roughly 1 in every 6 customers have had a valid transaction declined in the past year.[8]

The problem with data privacy

Many institutions are looking towards Machine Learning (ML) and Artificial Intelligence (AI) as a way of transforming their financal crime controls. A report released by the World Economic Forum and Deloitte in 2018 showed that the continued development of AI will radically alter the front and back office operations of financial institutions.[5]

But this is problematic in a world where consumer privacy is ever-more paramount. Machine learning, the basis of AI, involves algorithms that progressively improve themselves by using data; the more data they consume, the better they get at spotting patterns.

Whilst banks need to train their AI systems to better detect financial crime, under current privacy regulations like GDPR, they are restricted from using even their own customer data. Where this kind of sensitive data is concerned, people must give their explicit consent to its processing, thus hindering machine learning.

Reconnaissance

Attackers are willing to put a significant number of hours into collecting personal information for banking employees and identifying those responsible for the systems they're looking to manipulate. They may wait for weeks or even months before launching an attack, after testing for weaknesses in fraud controls. Due to the static nature of today's financial crime controls, they fail to detect this adaptive behaviour of criminals.

Lack of collaboration

AML detection is a dynamic process that requires awareness and consideration of transactional security issues, public policy, and the regulatory climate – areas simply not being incorporated into these AI scenarios.[6]

Criminals use money laundering techniques to disguise money from law enforcement authorities (LEAs) to increase their profits or to finance criminal or terrorist activities. Regulators are aware of this situation and have relied heavily on the international 40 FATF recommendations to tackle the problem. These 40 recommendations are being evaluated periodically in each country as part of the mutual evaluation report (MER).

Unfortunately, Anti-Money Laundering (AML) is being hampered by the lack of coordinated efforts between the LEAs, financial sector and academia. There are many roadblocks for researchers to get access to financial data, and regulations like GDPR are making things harder and more complex. An approach is needed to produce better policies that can be implemented by financial institutions.

The hidden fraud problem

Alongside all the challenges we've outlined in the previous section, there is one significant problem that permeates it all: hidden fraud.

Current fraud control methods focus only on two things to measure the improvement: reducing the number of innocent people wrongly tagged (False Positives) and 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 completely unknown. Only once we have generated information about the missing fraud can we start to improve financial controls effectively and reduce the cost.

Summary

The hidden fraud problem leads to several other drawbacks for financial institutions facing the task of effectively and efficiently detecting fraudulent activities:

- Historical data is not rich enough to develop better controls.
- Data privacy has restricted personal data use.
- Criminals are more adaptive than financial institutions, so the race is unfair.
- There are not enough diverse known cases of categorised financial crime data to fine-tune controls.
- There are too many false positives, because criminals disguise themselves among regular clients.

> “ ——— There is an inherent problem in developing better controls in the financial fraud domain. The main issue relies on the unknown metric of the total population of fraud. Without a clear measure of this, current fraud detection methods rely only on reducing the implementation cost.”

DR. EDGAR LOPEZ-ROJAS, FRAUD ANALYTICS EXPERT[10]

3.0

Simulation as a solution

Despite the many issues with traditional detection systems, there is a solution that has proven to be indispensable to tackling several real-world challenges for preventing and detecting financial crime: simulation.

By using a method called agent-based modelling (ABM), organisations can explore diverse and rich scenarios of fraud which would otherwise be challenging or unattainable, even with access to real data.

Regulators have recently confirmed that they will be using synthetic data as a solution to improve their approach to testing.[4] They will also expect firms to monitor the effectiveness of their own systems and explore RegTech solutions to tackle financial crime. By using simulation, firms can prove they have the capacity and capability to provide these regulators with quick access to data and systems.

Agent-based simulation for uncovering financial crime

Agent-based modelling is a bottom-up modelling approach, where the high-level properties of a system are generated from the low-level interactions of its constituents, or agents. An agent can be used to represent just about anything, including customers, fraudsters and merchants.

ABMs can generate emergent phenomena of the type that characterise Complex Adaptive Systems (CAS), such as cities and financial markets. These models provide us with large and rich parameter spaces which we can use to explore ‘what-if’ scenarios.

For example, banks can use the agent-based framework to evaluate and improve their current fraud detection systems.

With agent-based simulation, organisations can label all instances of fraud and measure the False Negatives to calculate metrics of performance, such as precision and recall. Only through this method can businesses measure the real improvement of their control system and reduce the ratio of undetected criminals.

Generating realistic synthetic datasets

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. Financial simulation is a novel and valid approach which involves the use of simulators to produce synthetic data.[11]

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. Synthetic datasets with labelled crime can be used by financial companies and regulators to assess the effectiveness of their transaction monitoring systems. This unique benchmarking capability has the advantage of measuring undetected or 'hidden' financial crime.[11]

Summary

By simulating millions of potential scenarios, financial institutions can create synthetic data that is essential to identifying labelled fraud that isn't being picked up by current systems. This simulated environment is quick and cost-effective and most importantly uses a non-private, non-personal synthetic version of customer data – so it's completely compliant with GDPR and other regulations.

4.0

Benefits to simulating financial crime analytics

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

Testing and training

With simulation, banks can anticipate the future before it happens by testing and training algorithms. By using synthetic and forensic data enriched by a realistic simulation they can control financial crime by:

- Developing new techniques to measure the efficacy of current and new fincrime detection techniques. They can compare results with current methods within diverse scenarios and generate diverse methods using an individual scenario.
- Measuring hidden crime that has remained undetected historically by applying new synthetic data sets and models that follow the dynamics of known crime.
- Anticipating the future using synthetic data within a realistic complex adaptive environment, since historic data only carries past patterns.

Minimise risk and reduce cost

Banks can use agent-based simulation to minimise risk while reducing cost by:

- Assessing and identifying key weaknesses and putting in place cost effective countermeasures.
- Accurately measuring the cost of visible fincrime and hidden fincrime.
- Proactively preparing for and using precisely the right approach to minimise the cost and risk for future financial crime.
- Demonstrating to regulators that they have the appropriate controls in place to better detect and prevent financial crime.

Adapt to change

Simulation empowers financial institutions to adapt and scale to address changes across both criminal behaviour and suspicious activity, as well as the evolving regulatory environment, by:

- Understanding future crime before committing valuable resources.
- Protecting clients from arbitrary, costly and ineffective fraud controls.
- Simulating expected scenarios before they happen and can impact balance sheets— in essence, future proofing their businesses from black swan activity.

Future-proof systems

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

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

A collaborative approach

Only through the use of simulation and generation of synthetic financial datasets can the financial sector better coordinate with LEAs and academia to improve AML policies worldwide. The ultimate aim is to create positive feedback loops between all three parties to improve detection methods (a framework termed the “Triple Helix Model” by Dr. Edgar Lopez-Rojas).[12]

By testing controls and understanding potential future attacks and entry points, organisations, LEAs and academics can make learn the best and most cost-effective decisions in a virtual environment before committing resources in the real world.

“ Simulation has been among us for several years and today, we have the technology, the computational power and the knowledge to use it as a powerful weapon in the fight against financial fraud. We are now able to generate information about False Negatives and help organisations move from a reactive to a proactive approach to fraud analytics.”

DR. EDGAR LOPEZ-ROJAS, FRAUD ANALYTICS EXPERT[10]

4.0

Implementing a solution

As with any innovation or transformation initiative, preparing for a pilot requires intensive research and due diligence on both internal processes and the chosen vendor. Early adopters recommend the following approach to implementing a solution.

Choosing the right vendor

Different organisations have different levels of readiness for a pilot, but ahead of any fincrime analytics simulation programme they should consider the following areas:

- Business problem: Has the internal problem been sufficiently articulated and have the relevant internal stakeholders been informed?
- Process: Is there a process in place to select a vendor?
- Data: Is there an internally sourced customer transactional dataset that can be used to generate a synthetic dataset?
- People: Are there people internally who understand the value of simulation, and do they have the capacity to work with the vendor to create a desirable outcome?
- Future: Is there a plan to extend the project beyond the pilot phase to continuously self-evaluate and improve fincrime controls?
- Leadership: Does the organisation trust simulation for fincrime analytics, and is there buy-in with an allocated budget?

Calibration

Calibration is an optimisation process that aids in model design, estimation and validation with respect to the statistical properties of real-world data and any behavioural dynamics of interest. A model's ability to reproduce realistic behaviours and the dynamics that generate these behaviours is dependent on quality calibration. A chosen vendor should use a validation process to ensure that the model design and parameters reproduce statistical and behavioural dynamics that match real-world data.

5.0

Conclusion

Today, we are woefully ineffective at preventing money laundering, as evidenced by the increasing number of banks being fined for failing to detect criminal activity. There are many reasons current fraud control systems are failing.

- Rules-based transaction monitoring: Traditional rules-based transaction monitoring causes a high rate of false positives, sometimes as high as 10-15%.
- Privacy regulations like GDPR: Under current privacy regulations, banks are restricted from using even their own customer data to improve their fincrime detection systems.
- Evolving criminal behaviour: The static nature of today's controls means they often fail to detect the adaptive and evolving behaviour of criminals.
- Lack of collaboration: AML initiatives are being hampered by the lack of coordinated efforts between the LEAs, financial sector and academia.
- The hidden fraud problem: Current systems do not consider the False Negatives, or undetected criminals, because this information is completely unknown.

An agent-based approach introduces an entirely new way of managing financial crime analytics. Instead of looking backwards at historical data, simulation can be used to generate synthetic transaction data that resembles real-world data. This type of data set can be used in a sandbox environment for many diverse purposes such as to train detection agents, test current methods and evaluate transaction monitoring systems.

Looking to the future

Once a firm is certain of measuring the improvements of detection algorithms, the team can simulate diverse scenarios by modifying the parameters, adding new typologies, and adding more labelled crime to properly train classifiers. These diverse scenarios can be evaluated against multiple controls using scorecard metrics, allowing an organisation to prepare for both current and future threats.

As criminals get ever more sophisticated at targeting permeable controls, simulation holds the key to winning the battle against financial crime.

6.0

Wider reading

From a commercial perspective, we are still in the early stages of using simulation to tackle financial crime. However, there are several research projects that have touched on the issue over the past decade which we recommend for wider reading.

2012: “Money Laundering Detection using Synthetic Data” (Lopez-Rojas and Axelsson).[13] This paper highlights the problem of obtaining financial datasets and proposes using synthetic datasets based on simulation.

2013: “Synthetic Logs Generator for Fraud Detection in Mobile Transfer Services” (Gaber et al.).[14] This study looks at generating testing data from a mobile transfer service that researchers can use to evaluate different approaches to fraud detection.

2013-2015: “RetSim Simulator and its Applications” (Lopez-Rojas, Edgar et al.).[15] Managing fraud is important for business, retail and financial alike. This work is based on the RetSim simulator and highlights several applications such as triage thresholds and measuring the cost of fraud in the domain of retail stores.

2014: “BankSim: A Bank Payment Simulation for Fraud Detection Research” (Lopez-Rojas et al.).[11] BankSim is an agent-based simulator of bank payments based on a sample of aggregated transactional data provided by a Spanish bank. The main purpose of BankSim is the generation of synthetic data that can be used for fraud detection research.

2015: “IncidentResponseSim: An Agent-Based Simulation Tool for Risk Management of Online Fraud” (Gorton).[16] This paper presents a simulation tool that supports the risk assessment of online banking services. It uses the power of simulation to estimate the economic consequences of current and emerging threats.

2016: “Applying Simulation to the Problem of Detecting Financial Fraud” (Lopez-Rojas, Edgar).[17] This PhD thesis presents an approach towards the use of computer simulation for fraud detection and its applications in financial domains such as retail stores and mobile money.

2018: “Analysis of Fraud Controls using the PaySim Financial Simulator” (Lopez-Rojas et al.).[18] PaySim is a financial simulator that simulates mobile money transactions using agent-based modelling, and has been widely used by students, practitioners and institutions since publication.

2018: “On the GDPR in EU and its Impact on Financial Fraud Research” (Lopez-Rojas).[19] This paper aims to analyse the impact of GDPR from the financial services perspective regarding the handling of personal data.

2019: “Triple Helix approach for Anti-Money Laundering (AML)” (Lopez-Rojas et al.).[12] The aim of the framework is to produce positive feedback loops between LEAs, academia and organisations to improve fraud detection methods.

2019: “Advantages of the PaySim Simulator for Improving Financial Fraud Controls” (Lopez-Rojas et al.). [20] This paper presents the work of researchers who have had access to data leverage a real-life scenario based on a known fraud scheme to demonstrate the advantage of simulated data over real-world data when setting adequate controls for fraud detection.

7.0

About Simudyne

Simudyne is the market leader in agent-based financial simulation supporting advanced fincrime analytics. A partnership with Simudyne ensures your organisation has the industry's most advanced fincrime 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 fincrime 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.

Why Simudyne?

- A base model to develop an advanced capability in training and testing fincrime 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.

REFERENCES

1 Brian Monroe, “Global Cost of Fraud Tops £3 Trillion”, Accountancy Daily, May 2018, https://www.accountancydaily.co/global-cost-fraud-tops-3-trillion, accessed April 22, 2019.

[2] Sarah Min, “Fraud Takes Over as Consumers Top Complaint to FTC”, March 2019, https://www.cbsnews.com/news/fraud-takes-over-as-consumers-top-complaint-to-ftc/, accessed April 23, 2019.

[3] Internal source.

[4] EY, “What the FCA Business Plan 2019/20 Means for your Firm”, April 2019, accessed April 30 2019.5 Deloitte, “The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing”, 2018, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf, accessed April 20, 2019.

[5] Deloitte, “The Case for Artificial Intelligence in Combating Money Laundering and Terrorist Financing”, 2018, https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/finance/sea-fas-deloitte-uob-whitepaper-digital.pdf, accessed April 20, 2019.

[6] Joshua Fruth, “Anti-money laundering controls failing to detect terrorists, cartels, and sanctioned states”, March 2018, https://www.reuters.com/article/bc-finreg-laundering-detecting/anti-money-laundering-controls-failing-to-detect-terrorists-cartels-and-sanctioned-statesidUSKCN1GP2NV, accessed April 24, 2019.

[7] Roy Wedge et al., “Solving the False Positives Problem in Fraud Prediction Using Automated Feature Engineering”, September 2018, http://www.ecmlpkdd2018.org/wp-content/uploads/2018/09/567.pdf, accessed April 13 2019

[8] Guardian Analytics Financial Crimes Team, https://guardiananalytics.com/how-improved-fraud-prevention-increases-operational-efficiencypart-4-in-a-4-part-series/, accessed April 24, 2019.

[9] Yalman Onaran,“Stung by Big Fines, Big Banks Beef Up Money-Laundering Controls”, March 2018, https://www.bloomberg.com/news/articles/2019-04-04/global-banks-beef-up-money-laundering-controls-as-fines-sting, accessed April 23, 2019.

[10] Lopez-Rojas, Edgar Alonso; Elmir, Ahmad; Axelsson, Stefan. PaySim: A financial mobile money simulator for fraud detection Inproceedings. The 28th European Modeling and Simulation Symposium-EMSS, Larnaca, Cyprus, 2016.

[11] Lopez-Rojas, Edgar Alonso; Axelsson, Stefan. Banksim: A bank payments simulator for fraud detection research Inproceedings. 26th EuropeanModeling and Simulation Symposium, EMSS 2014, Bordeaux, France.

[12] Lopez-Rojas, Edgar A; Zoto, Erjon. Triple Helix Approach for Anti-Money Laundering (AML) Research Using Synthetic Data Generation Methods Inproceedings. The 10th International Conference on Society and Information Technologies: ICSIT 2019.

[13] Lopez-Rojas, Edgar Alonso; Axelsson, Stefan. Money Laundering Detection using Synthetic Data Inproceedings.Bidot, Julien Karlsson Lars ;(Ed.): The 27th workshop of the Swedish Artificial Intelligence Society (SAIS), pp. 33–40, Linköping University Electronic Press, Örebro, 2012.

[14] Gaber, Chrystel & Hemery, Baptiste & Achemlal, Mohamed & Pasquet, Marc & Urien, Pascal. (2013). Synthetic Logs Generator for Fraud

Detection in Mobile Transfer Services. Proceedings of the 2013 International Conference on Collaboration Technologies and Systems, CTS 2013. 7859.10.1109/CTS.2013.6567225.

[15] Lopez-Rojas, Edgar Alonso; Axelsson, Stefan; Gorton, Dan. RetSim: A Shoe Store Agent-Based Simulation for Fraud Detection Journal Article. The 25th European Modeling and Simulation Symposium, Athens, Greece, 2013.

[16] Gorton, Dan. (2015). IncidentResponseSim: An Agent-Based Simulation Tool for Risk Management of Online Fraud. 9417. 10.1007/978-3-319-26502-5_12.

[17] Lopez-Rojas, Edgar Alonso. Applying Simulation to the Problem of Detecting Financial Fraud PhD Thesis. Blekinge Institute of Technology,2016.

[18] Lopez-Rojas, Edgar Alonso; Axelsson, Stefan ; Baca, Dejan. Analysis of fraud controls using the PaySim financial simulator Journal Article. International Journal of Simulation and Process Modeling, 13 (4), pp. 377-386, 2018.

[19] Lopez-Rojas, Edgar Alonso; Gultemen, Dincer; Zoto, Erjon. On the GDPR introduction in EU and its impact on financial fraud research Inproceedings. The 30th European Modeling and Simulation Symposium-EMSS, Budapest, Hungary, 2018, ISBN: 978-88-85741-03-4.25

[20] Lopez-Rojas, Edgar Alonso; Sani, Amir; Barneaud, Camille. Advantages of the PaySim Simulator for Improving Financial Fraud Controls. Norwegian University of Science and Technology, 2019.

Contact

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.