Advantages of the PaySim Simulator for Improving Financial Fraud Controls

Edgar A. Lopez-Rojas[1,2] and Camille Barneaud[3]

[1] Norwegian University of Science and Technology (NTNU)
edgar.lopez@ntnu.no,
WWW home page: http://edgarlopez.net
[2] Simudyne [edgar,amir]@simudyne.com,
WWW home page: http://simudyne.com
[3] Flaminem camille.barneaud@flaminem.com,
WWW home page: http://flaminem.com

Abstract. Financial transactions lay up the foundation of modern society. Unfortunately, illicit abuse of the financial system is pervasive. Fraud controls aim to detect these suspicious activities, but they require deep analysis to model their efficacy and value proposition. Due to the private nature and scale of these financial transactions, this analysis is often performed in hindsight. Financial institutions lack of information, due to *the hidden fraud problem*, to properly set and tune their fraud controls systems. This is probably one of the reasons we are losing the war against crime. This paper presents PaySim, a cutting edge agent-based model that simulates financial fraud scenarios to improve current fraud controls. PaySim uses aggregated anonymized data from a real financial dataset to generate synthetic data that closely resembles the transactions dynamics, statistical properties and causal dynamics observed in the original dataset, while incorporating any malicious behaviour of interest. Using an agent-based framework specifically designed to cover the demands of financial simulation and the application of mathematical statistics, we 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.

Keywords: Multi-Agent-Based Simulation; MABS; Financial Fraud; Mobile Money; Fraud Detection; Synthetic Data; Agent-Based Modeling; Multi-agent Systems; Reinforcement Learning; Machine Learning

1 Introduction

As economies continue to move from analogue to digital economies, they become more accessible and often more vulnerable to breaches. Financial fraud controls are insufficient to stop the wrongdoers. In fact, many are simply focused on meeting minimum legal requirements. Around 90% of Europe's largest banks have been sanctioned for money laundering, and the number of fraud cases just keep growing world wide. Some examples of this phenomenon includes HSBC in

Mexico[1], Swedbank, Nordea and Handlesbanken in Sweden[2] and more recently the case of ING in the Netherlands[3]. On top of that there are several difficulties for researchers that work on fraud controls, both from academia and industry to get access to financial data due to the private nature of it. These restrictions are increasing with the recent introduction of GDPR and its implication in financial fraud research [4].

Criminals are getting more sophisticated at targeting institutions' permeable controls and weakest links. Privacy is critical as fines are ever more frequent as breaches continue to accelerate. On the other hand there are promising technologies that are showing remarkable progress in the area of fraud control such as machine learning. However, machine learning and AI are restricted from using personally identifiable data as a result of restrictions such as GDPR.

This paper presents PaySim, a cutting edge agent-based model that simulates financial fraud scenarios to improve current fraud controls. PaySim uses aggregated anonymised data from a real financial dataset to generate synthetic data that closely resembles the transactions dynamics, statistical properties and causal dynamics observed in the original dataset, while incorporating any malicious behaviour of interest. Using an agent-based framework specifically designed to cover the demands of financial simulation and the application of mathematical statistics, we 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.

The intended audience for the paper are those who are in need to have a tool for collaborating between restricted financial domains and researchers who lack valuable data. This research can also benefit people working with financial service institutions, financial regulators, academic institutions and similar related industries. Any organisation that wants an alternative method to share financial information and avoid GDPR barriers may also interested in this work because it enables access to "advanced modelling techniques" that allow them to model feasible scenarios for testing and measuring their fraud controls methods.

[1] HSBC fined with 1.9 Billions USD for money laundering in 2012. https://www.bbc.com/news/business-20673466

[2] Swedbank 2019 https://www.swedbank.com/about-swedbank/information-on-tv-reports-on-money-laundering.html. Nordea and Handelsbanken are fined with 50m SEK and 35m SEK in 2015. https://www.reuters.com/article/nordea-bank-handelsbanken-fsa/update-1-nordea-handelsbanken-fined-over-money-laundering-breaches-idUSL5N0YA1MS20150519

[3] ING fined with 700m USD for money laundering in 2018. https://www.reuters.com/article/us-ing-groep-settlement-money-laundering/dutch-bank-ing-fined-900-million-for-failing-to-spot-money-laundering-idUSKCN1LK0PE

2 Background and Context

The concept of financial simulators has been developed earlier to create models of financial markets and financial forecasts [1, 11, 12]. Simulation has also been applied to solve cyber-security problems [2].

After the enforcement of GDPR in late May 2018, many organisations are interested in new methods that either comply with or avoid handling personal information. Simulation has the potential solution to this, by enabling sharing without disclosure of personal data. Financial simulation is a novel and valid approach in financial fraud analytics which involves the use of simulators to produce a sufficient level of financial data containing both the normal and the fraudulent behaviour [7, 6, 14]. Using simulators and the generated synthetic datasets enables researchers to have a test environment for developing the required controls.

Recent studies suggest that there is a need for better data to properly address the evaluation and status of fraud controls to complex problems such as Anti-Money Laundering, better known as AML [3]. The majority of policies and controls are based on classic computational controls such as thresholds. However, there is a body of research that shows that novel techniques such as machine learning can benefit from using synthetic data generation methods to target more accurately and efficiently suspicious transactions [13].

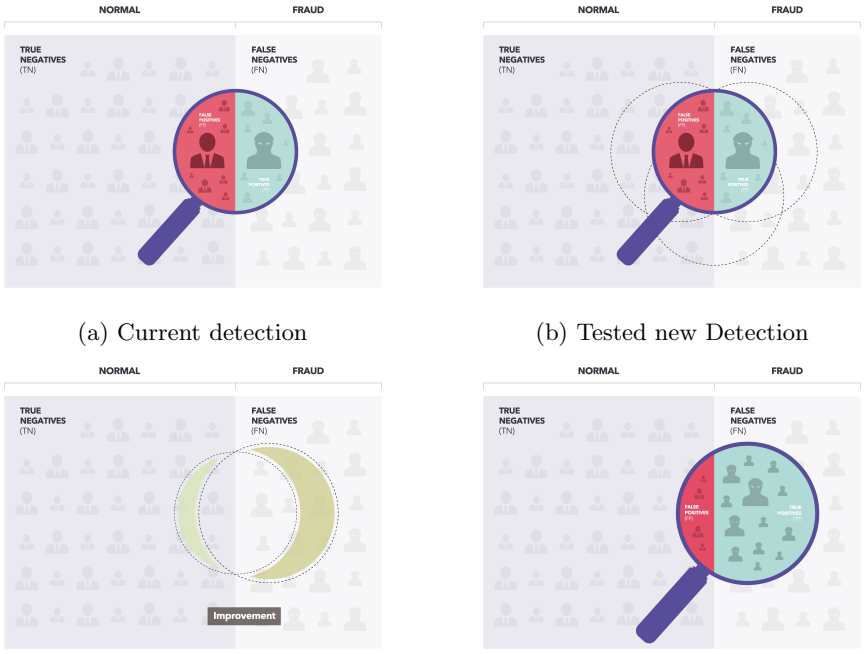
Financial simulation can be the key to unlock the synergies and mitigate the barriers for cooperation between Academia, the Financial Sector and the Government by using simulation as the central tool to bridge the parties. Through models such as the triple helix model for AML (TH-AML) we can address in a collaborative way complex problem such as money laundering [10].

3 The Problem of Developing Better Fraud Controls

There is an inherent problem to develop 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 only rely on improving the false positives and the true positives. Reducing the false negative rate is also a desirable measure of improvement in a dynamic and constantly changing fraudulent environment.

In Fig. 1(a) we represent the current status of a fraud detection method inside a financial institution. The whole area represents the whole universe of transactions. For improving fraud controls financial institutions aim to efficiently minimise fraud risk while reducing cost by reducing the cases of false negatives and at the same time aiming to comply with regulators. But a real improvement of the detection system should be in the direction of reducing the total fraud as depicted in Fig. 1(b and c). At the moment, the total value of fraud (FN+TP) is unknown.

From Fig. 2 we can see that from the two more relevant metrics for fraud detection, only Precision (1) is computable for financial institutions. Recall (2) uses the false negative (FN) to compute which is the hidden fraud. This gives



(a) Current detection

(b) Tested new Detection

(c) Measure the improvement

(d) Implement new method

Fig. 1: Visualisation of a fraud control improvement

only half of the equation for combined metrics such as the Harmonic F-score (3) which balance the weight to Precision and Recall or the F-score using beta (4) which gives more weight to either Precision or Recall. This gives the possibility for a financial institution to define an objective function that realistically fights the crime while considering the resources of the organisation.

$$Precision = \frac{TP}{FP + TP} \tag{1}$$

$$Recall = \frac{TP}{FN + TP} \tag{2}$$

$$F_2 = 2 * \frac{Precision * Recall}{Precision + Recall} \tag{3}$$

$$F_{score} = (1 - \beta^2) * \frac{Precision * Recall}{\beta^2 * Precision + Recall} \tag{4}$$

The *hidden fraud problem* adds up to several other drawbacks that financial institutions are facing at the moment when facing the task of effectively and efficiently detect fraudulent activities.

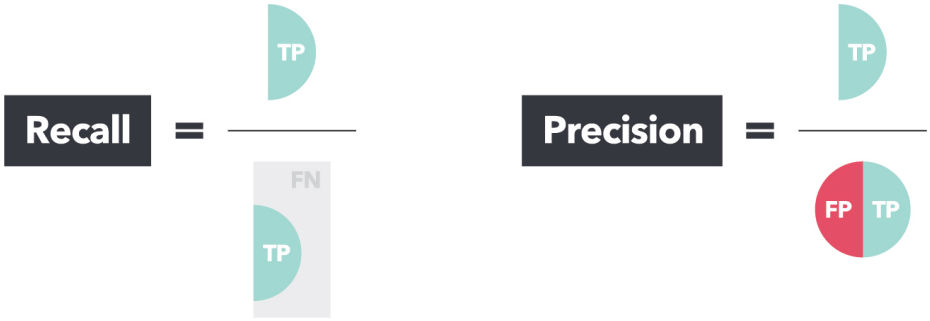


Fig. 2: Recall and Precision visually explained

Some of the drawbacks of current fraud control techniques can be summarised as:

- Historical data is not rich enough to develop better controls.
- Data privacy has restricted personal data use therefore restricting the potential for third parties to help in the problem.
- Fraudsters are more adaptive than financial institutions, so the race is unfair.
- There are not enough diverse known cases of categorised fraud data to tune fraud controls.
- There are far too many false positives, because criminal aim to disguise themselves among regular clients.

In this paper we argue that simulation provides a set of advantages for the task that financial institutions have of detecting fraud activity.

Some of the advantages of using simulation for implementing fraud control can be summarised as:

- Assessing and identifying key weaknesses and putting in place cost effective countermeasures.
- Accurately measuring the cost of visible fraud and hidden fraud.
- Proactively preparing for and using precisely the right approach to minimise the cost and risk for future fraud.
- Anticipate the future before it happens by testing and training up their approach.
- By using synthetic and forensic data enriched by a realistic simulation they can experiment with fraud behaviour in a controlled environment.
- Rapidly adapt and scale to address changes across both fraudulent behaviour and suspicious activity as well as the evolving regulatory environment.

4 PaySim Demo

In this demo we would like to show how the PaySim [9] simulator is used to generate synthetic datasets based on real world datasets of financial data to study

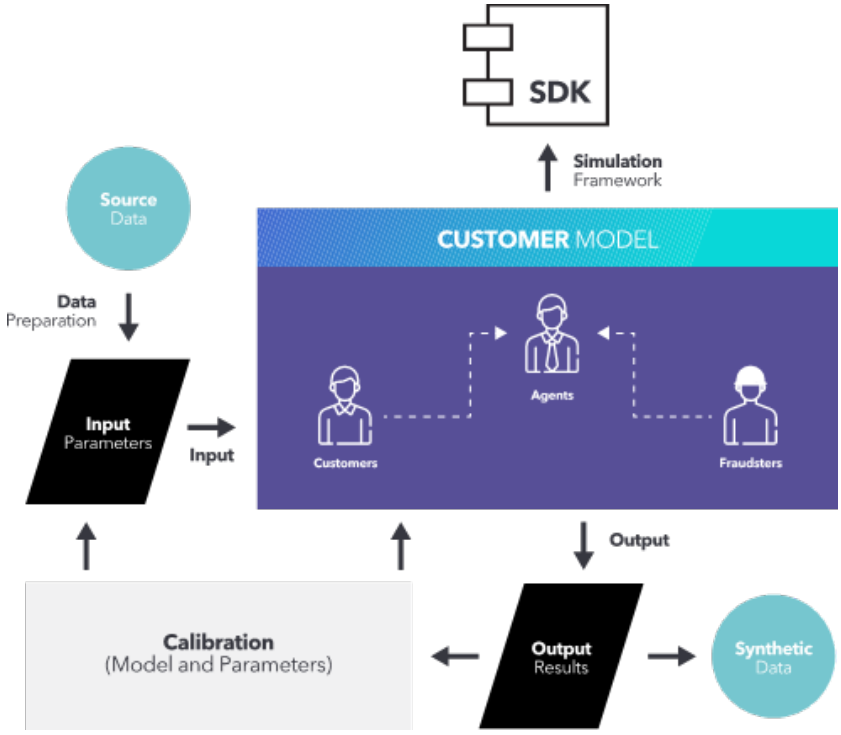


Fig. 3: Simulation Process of PaySim

and perform research on fraudulent financial schemes such as money laundering and terrorism financing to evaluate the effectiveness and impact of diverse controls. By using synthetic datasets, the researchers have the opportunity to explore diverse and rich scenarios of fraud that would otherwise be challenging or unattainable even with access to real data.

The new version of PaySim uses an agent-based framework, specifically designed by to cover the functional and computational demands of financial simulation with the explicit purpose of developing fraud analytics. The way it works is depicted in Fig. 3. It uses real data to calibrate the required parameters that allow the generation of synthetic datasets. Once the calibration satisfies the similarity comparison between the real and the synthetic data, we output synthetic datasets that are used to study fraud phenomenons and that contain labelled instances of generated fraud schemes. This process can be iterative and can be used to generate diverse scenarios of fraud or predictive future scenarios that otherwise are not present in the real data.

5 Results

The scenario selected is based on the fraud case presented in previous work [8] which happens when the client loses control and access to his/her account. The fraudster takes control and uses disposable mule accounts to transfer the money, and later cashes them out. All of this can only happen in a very short time, because when the clients discover that their accounts are compromised, the first action they should take is to contact customer service to block any possible further malicious transactions. We want to present a scorecard metric to evaluate which way we can achieve better performance of the fraud control.

The experiment introduces a 3% probability for each of the 1000 fraudsters to perform fraud at any given step of the simulation, which is perhaps an aggressive value (30 fraudulent activities per hour), but this helps to inject enough fraudulent activity to study the phenomenon.

In order to study this phenomenon, we ran the system four times increasing the maximum amount of transaction possible in a single TRANSFER each time. We selected four synthetic datasets that used the thresholds on transfer transactions of 300k (PS89745), 600k (PS80775), 900k (PS00273) and 1200k (PS98516). The first case obligates the fraudster to perform several operations to empty accounts that contains a balance above this threshold. The last limit is very flexible and allows the fraudsters to perform a single TRANSFER operation in most cases. By implementing an extra control that will temporarily block accounts that exceed three consecutive transfers for the maximum amount in a short period of time we could effectively reduce the amount of fraud and measure the benefit of this control. With the help of PaySim, we can also measure how other users will be affected by this block in their accounts (False Positives).

Table 1 shows the number of transactions type TRANSFER and the classification of fraud. The first obvious and important thing to notice is that whenever there is a control, the effort required for committing fraud gets higher. Just by introducing a lower threshold on the maximum amount allowed for a transfer, the number of transactions needed to empty an account increases several times. However, the number of legitimate users that will be affected increases. This is the trade-off in fraud detection that a manager needs to address in enacting the fraud controls. Table 1 also shows the loss due to fraud. If we focus attention on the False Negative (FN) row of each simulation, we can see the profit from fraud. The bigger the threshold the higher the profit. The task for a manager is to reduce this amount while minimising False Positives (FP) cases, which are legitimate customers that have their account blocked by the controls implemented to prevent fraud.

6 Discussion

Table 2 show the fraud detection results of each of the datasets evaluated here. We see that the precision is higher when the threshold is higher as in dataset

Table 1: Fraud Detection Classification

LogName	Class	Count	Amount	% count	% amount
PS89745 (300k)	FN	27,412	6,724M	1.005%	0.363%
	FP	982	214M	0.036%	0.012%
	TN	2,607,642	1,816,764M	95.579%	98.162%
	TP	92,211	27,076M	3.380%	1.463%
PS80775 (600k)	FN	24,400	11,291M	0.990%	0.581%
	FP	58	17M	0.002%	0.001%
	TN	2,396,684	1,907,409M	97.239%	98.126%
	TP	43,604	25,114M	1.769%	1.292%
PS00273 (900k)	FN	21,072	12,854M	1.024%	0.768%
	FP	8	1M	0.000%	0.000%
	TN	2,011,006	1,639,699M	97.712%	97.903%
	TP	26,006	22,264M	1.264%	1.329%
PS98516 (1200k)	FN	20,493	16,189M	0.921%	0.858%
	FP	1	0.168M	0.000%	0.000%
	TN	2,186,516	1,849,707M	98.215%	97.993%
	TP	19,248	21,686M	0.865%	1.149%

PS98516 (1200k). This means that we will have fewer customers affected. However, the recall is seriously affected, which means that the fraudsters will profit more using this control (16,189 million).

Table 2: Fraud Detection Results

LogName	Precision	Recall
PS89745	98.946%	77.085%
PS80775	99.867%	64.120%
PS00273	99.969%	55.240%
PS98516	99.995%	48.434%

On the other hand when we have a lower threshold as in *PS89745* (300k), the number of false positives (FP) increases to 982. But, we have a considerably higher recall which means that we lower the total value of fraud (6,724 million). The primary conclusion we have from using simulation is that we are able to measure any require metric to be able to improve the performance of fraud controls systems.

Financial institutions lack of information to properly set and tune their fraud control systems. This is probably one of the reasons we are losing the war against crime. From Table 1 we can see that by applying strict controls we are obtaining a high number of False Positives (982 in case of 300k). The opposite phenomenon

occurs when we apply very tolerant controls as in the case of 1200k threshold where we obtain only one FP. When we have strict controls the profit of the undetected fraud (False Negatives) is considerably less than when we have tolerant controls. However, the financial institutions lack of the knowledge of the False Negatives to properly tune their systems in an adequate way that satisfy not only the regulators but also decreases in a considerable way the profit from the criminal activities.

Simulation has limitations as presented in previous research [5]. We believe, simulation for financial fraud is not widely used at the moment because it is not a trivial task to produce a quality model and synthetic dataset. However, the shortcomings if properly handled are less than the advantages presented here.

7 Conclusions

The primary conclusion we have from using simulation is that we are able to measure any require metric such as the Precision and the Recall to be able to improve the performance of fraud controls systems. Financial institutions lack of the knowledge of the hidden fraud, which is in terms of fraud detection the False Negatives, to properly tune their systems in an adequate way that satisfies not only the regulators but also decreases in a considerable way the profit from the criminal activities.

By using financial simulators such as the PaySim simulator we are able to obtain enough information and explore diverse fraud scenarios to deliver a real improvement of fraud detection systems which will tackle both, the cost of the business due to miss classification and the reduction of the criminal profit.

At the moment we are able to produce realistic synthetic data and desirable future fraud scenarios to study the fraud phenomenon. Future work should focus on preparing simulation for easy sharing models and parameters as if they were word-processors documents to enable models such as the Triple Helix Approach for AML (TH-AML) mentioned earlier [10].

Acknowledgments

This work was sponsored by Simudyne (simudyne.com) London, UK.

References

1. B. Hedjazi, M. Ahmed-Nacer, S. Aknine, and K. Benatchba. Multi-agent financial market simulation: Evolutionist approach. *International Journal of Simulation and Process Modelling*, 8(2-3):185–199, 2013.
2. P. Legato and R. Mazza. A simulation optimisation-based approach for team building in cyber security. *International Journal of Simulation and Process Modelling*, 11(6):430–442, 2017.
3. Michael Levi, Peter Reuter, and Terence Halliday. Can the AML system be evaluated without better data? *Crime, Law and Social Change*, 2018.

4. Edgar A. Lopez-Rojas, Dincer Gultemen, and Erjon Zoto. On the gdpr introduction in eu and its impact on financial fraud research. In *The 30th European Modeling and Simulation Symposium-EMSS, Budapest, Hungary*, 2018.
5. Edgar Alonso Lopez-Rojas and Stefan Axelsson. Money Laundering Detection using Synthetic Data. In Julien Karlsson, Lars ; Bidot, editor, *The 27th workshop of (SAIS)*, pages 33–40, Örebro, 2012. Linköping University Electronic Press.
6. Edgar Alonso Lopez-Rojas and Stefan Axelsson. Banksim: A bank payments simulator for fraud detection research. In *26th European Modeling and Simulation Symposium, EMSS 2014*, pages 144–152. Dime University of Genoa, 2014.
7. Edgar Alonso Lopez-Rojas and Stefan Axelsson. A Review of Computer Simulation for Fraud Detection Research in Financial Datasets. In *Future Technologies Conference, San Francisco, USA*, 2016.
8. Edgar Alonso Lopez-Rojas, Stefan Axelsson, and Dejan Baca. Analysis of fraud controls using the paysim financial simulator. *International Journal of Simulation and Process Modeling*, 13(4):377–386, 2018.
9. Edgar Alonso Lopez-Rojas, Ahmad Elmir, and Stefan Axelsson. PaySim: A financial mobile money simulator for fraud detection. In *The 28th European Modeling and Simulation Symposium-EMSS*, Larnaca, Cyprus, 2016.
10. Edgar Alonso Lopez-Rojas and Erjon Zoto. Triple Helix Approach for Anti-Money Laundering (AML) Research Using Synthetic Data Generation Methods. In *The 10th International Conference on Society and Information Technologies: ICSIT 2019*, 2019.
11. Michael J. O'Loughlin, Mary K. Driskell, and Gregory Diehl. Financial simulation: Combining cost information in systems analysis. In *Winter Simulation Conference Proceedings*, pages 578–581, 1990.
12. T. Takaishi. Multiple time series ising model for financial market simulations. *Journal of Physics: Conference Series*, 574(1), 2014.
13. Dianmin Yue, Xiaodan Wu, Yunfeng Wang, Yue Li, and Chao-Hsien Chu. A Review of Data Mining-Based Financial Fraud Detection Research. In *2007 International Conference on Wireless Communications, Networking and Mobile Computing*, pages 5514–5517. Ieee, sep 2007.
14. Luisa Zintgraf, Edgar A Lopez-Rojas, Diederik Roijers, and Ann Nowe. Multimaus: a Multi-Modal Authentication Simulator for Fraud Detection Research. *In Proceedings of the European Modeling and Simulation Symposium (EMSS), September*, (c), 2017.