Institution: University of Greenwich		
Unit of Assessment: 11 - Computer Science and Informatics		
Title of case study: Informing Public Policy and Regulation with AI-based analysis for the detection of Money Laundering and Fraud		
Period when the underpinning research was undertaken: January 2012 – July 2020		
Details of staff conducting the underpinning research from the submitting unit:		
Name(s):	**Role(s) (e.g. job title):**	**Period(s) employed by submitting HEI:**
Georgios Samakovitis	Associate Professor, Enterprise Lead, School of Computing & Mathematical Sciences	01/09/2011 – present
Stelios Kapetanakis	Senior Lecturer, School of Computing & Mathematical Sciences	01/08/2011 – 05/07/2013
Period when the claimed impact occurred: August 2013 – July 2020		
Is this case study continued from a case study submitted in 2014? N		

1. Summary of the impact

Research led by **Dr Georgios Samakovitis** on fraud detection and anti-money laundering has resulted in multiple impacts related to financial services and their regulation. The nature of the impact is commercial-economic and public policy-related, with key beneficiaries being UK government, industry and financial services regulators, and society as end-users. The techniques and concepts introduced by **Samakovitis** had distinct material contribution to changing the perception of UK public bodies and the financial services industry, initially through attracting stakeholder interest in industry fora, and later through **Samakovitis**' direct contribution in the UK Payments Strategy Forum and the HMG Cabinet Office Counter-fraud Data Advisory Group.

More specifically, successful application of Case-based Reasoning (CBR) for fraud detection in electronic money transfer has proven that intelligent techniques that rely on prior knowledge (confirmed illicit transactions) mitigate costly misclassification risks borne by other, often more advanced, practices. Combined through an operational framework for secure transaction data sharing (the Collective Intelligence Hub – (CIH)), the above results provided "*strong evidence for regulators, payment service providers, and users that financial transaction sharing is both feasible within the required data privacy frameworks, and necessary to significantly enhance mitigation capabilities in Counter-Fraud*" **[5.3]**. The work was fractionally supported by Dr. Stelios Kapetanakis who departed from Greenwich in late 2013.

2. Underpinning research

The underpinning research stems from the development of intelligent automated methods and tools for identifying financial transactions fraud and, in so doing, facilitate users (financial institutions, policy makers and regulators) to inform their approach and policies in investigating illicit money exchange. Tested on different financial transaction datasets, the research highlighted the capability to leverage characteristics of previously identified fraud to automate detection by predicting patterns of such illicit exchange; this further demonstrated the significant practical value that AI techniques carry, in informing decisions on counter-fraud and anti-money laundering policy. The work highlights early use of AI techniques to structure financial transaction data, which has uncovered patterns of mechanisms that informed regulations. Even though the specific AI techniques used (CBR) may not scale-up as well as more recent AI and Data Science techniques, it is the heuristic contributions, in terms of pattern detection that made it possible to inform regulations. These heuristics will outlast the use of a specific AI technique, notwithstanding the fact that CBR maintains an advantage in terms of representation semantics over techniques that have since gained greater popularity.

The earlier research **[3.1]** presented a prototype system introducing a workflow approach to identify abnormal financial transactions by applying CBR (Case Based Reasoning, an Artificial

Intelligence approach) for transactions classification. The approach features characteristics which are directly usable in fraud and money laundering identification, such as the construction and representation of integrated cases from transaction data and its ability to derive and leverage case similarity as a critical identifier of suspected fraud. Grounded on results of the above research, **[3.2]** then proposed an intelligent Financial Fraud Detection framework and architecture that acts as both an analytical and policy model for anonymised financial transaction data sharing.

On a parallel research stream, impact was underpinned by work **[3.1**, **3.3]** investigating the use of Case-based Reasoning (CBR) for identifying fraudulent transactions in mobile money transfer systems **[3.1]** and credit card transactions **[3.3]**. In particular, work in **[3.3]** focused on the development and testing of CBR techniques to detect fraudulent transactions with pre-classification of proven fraud cases, which succeeded in predicting a significant part of unknown fraud cases. The research offered a tool at a proof-of-concept level that is testable on real transaction datasets. The work described in **[3.3]** above expanded in scope to investigate transaction fraud in mobile money transfer (MMT) thus addressing an area of significant exchange value (presently at $130bn, expected to grow to $203bn by 2024), especially at a time where MMT forms the core mechanism for Peer-to-peer (P2P) and so-called Social Payments, which accounted for approximately 80% of transactions globally in 2019, according to Juniper Research. Similarly, the research in **[3.4]** underpins impact through investigating the novel use of combined artificial intelligence approaches (natural language processing, CBR and deep learning) to detect social engineering in networks; the proposed model delivers high accuracy in detecting attacks, and is tested on real data. The approach's underlying significance is in its potential use for critical support for payment networks; especially where money transfer occurs without financial intermediation (P2P), the proposed model can deliver important insights to users on potential malicious adversarial activity. In turn, its particular significance is largely reflected by the present and projected future growth figures in peer-to-peer (P2P) money transfer discussed above.

At the operational and policy levels, the research **[3.2**, **3.3]** highlighted the critical role of technological architectures for secure cross-institution privacy-preserving data sharing for anti-money laundering, proposing "*the establishment of an independently commissioned Collective Intelligence Hub as the infrastructure and governance framework guaranteeing synergistic intelligence against money laundering networks"* **[5.2]**; at the technological level (computational intelligence), the research developed, tested and reviewed knowledge engineering and machine learning techniques in anti-money laundering, fraud prediction in financial transactions, and social engineering. At that same technological level, later research by **Samakovitis** investigated applications of Distributed Ledger Technologies (DLTs – blockchain) for privacy preservation and transaction auditability. Notably, during the impact period (and particularly post-2017), emergent blockchain solutions challenged the incumbent technological paradigm in data sharing, across multiple areas of intelligent data analysis (not excluding fraud, identity verification or privacy preservation). However, it is important to highlight that, despite such disruptive barriers, the technological and operational framework underpinning the Collective Intelligence Hub (CIH) proposition is far from obsolesced through DLT, because of *"the critical requirement for control and oversight by a centralised delegated authority*" **[5.2]**. Conversely, several technological components of the CIH may arguably be improved with blockchain technologies, albeit not challenging its core operating principles. This is further evidenced by the present industry trajectory in the UK, where Vocalink, the operator of BACS, FPS and LINK in the country, has been developing network-wide counter fraud solutions along the same principles of centralised oversight as these recommended in the CIH (see indicatively https://www.vocalink.com/services/financial-crime-solutions/).

3. References to the research

1. Adedoyin A., Kapetanakis S., **Samakovitis G.**, Petridis M. (2017) Predicting Fraud in Mobile Money Transfer Using Case-Based Reasoning. In: Bramer M., Petridis M. (eds) Artificial Intelligence XXXIV. SGAI 2017. Lecture Notes in Computer Science, vol 10630. Springer, Cham. https://doi.org/10.1007/978-3-319-71078-5_28

Work in **[3.1]** was disseminated in the BCS Specialist Group in Artificial Intelligence (SGAI) conference and received the Best Paper award in the event's Application Stream in 2017.

2. **Samakovitis, G.** and Kapetanakis, S. (2013), Computer-aided Financial Fraud Detection: Promise and Applicability in Monitoring Financial Transaction Fraud, Proceedings of the International Conference in Business Management and Information Systems, (ICBMIS 2013) Nov. 19-21, Dubai, United Arab Emirates. https://gala.gre.ac.uk/id/eprint/17237/
   The work in **[3.2],** presenting a proposition for counter-fraud systems architectures, focuses primarily on the policy-related aspects of the recommended model (rather than on its technical feasibility) and, as such, was disseminated to a venue which, while not core to the relevant Unit of Assessment, allowed for the necessary visibility to how the proposed Collective Intelligence Hub solution can be modelled and commercially operationalised.
3. Kapetanakis, S., **Samakovitis, G.**, Gunasekera, B. and Petridis, M. (2012), Monitoring Financial Transaction Fraud with the use of Case-based Reasoning, Seventeenth UK Workshop on Case-Based Reasoning (UKCBR 2012) 11th December 2012, Cambridge, UK. https://gala.gre.ac.uk/id/eprint/9780/ [Full text available from university on request]
   Work in **[3.3]** that formed the grounds for investigating the uses of Case Based Reasoning (CBR) in fraud detection, was disseminated in the specialist workshop (UKCBR) which is part of the SGAI conference and the key CBR-specialist venue in the UK.
4. Lansley, M., Polatidis, N., Kapetanakis, S., Amin, K., **Samakovitis, G.**, and Petridis, M. (2019). Seen the villains: Detecting Social Engineering Attacks using Case-based Reasoning and Deep Learning. In Workshops Proceedings for the Twenty-seventh International Conference on Case-Based Reasoning co-located with the Twenty-seventh International Conference on Case-Based Reasoning (ICCBR 2019), http://ceur-ws.org/Vol-2567/paper4.pdf
   Work presented in **[3.4]** was disseminated in the International Conference in Case Based Reasoning (ICCBR), which has a Core B ranking (http://portal.core.edu.au/conf-ranks/).

4. Details of the impact

Underpinning research work, "*presented to a wide range of payment professionals and officials informed and, to an extent, influenced that subsequent work – both in government and in the payments industry – on data sharing for the combatting of public sector fraud and money laundering*" **[5.2]**. Specifically, the impact of the underpinning research is visible across commercial and public policy, through **(1) informing the UK Financial Services industry strategy for electronic payments**, **(2) influencing policy discussions on countering fraud and money laundering practices,** which shaped the Payment Regulators' position, and; **(3) informing the perception of government stakeholders and policymakers on how data sharing strategies, especially pertaining to financial fraud and money laundering practices, can improve Civil Service operation,** via direct advisory contribution with the HMG Cabinet Office. Further societal impact materialised through **(4) motivating the public debate on counter-fraud among beneficiaries, including the citizen as end-user of financial services.**

The underpinning work, carried out from 2012 to 2020, focused on enhancing the performance of counter-fraud and Anti-Money Laundering regimes through collaborative models grounded on Artificial Intelligence (AI) and data analytics. The impact of this has primarily taken the form of influence on UK public policy and regulation, informing the public and industry debate on technologies and approaches for counter fraud and anti-money laundering in the UK, **[5.5 – 5.9]** and informing the introduction of policies which, in turn had an impact on economic growth.

The research came at a time (2013) well-predating UK regulators' efforts to encourage or support such models, which later became mainstream, as also witnessed by the relevant New Payment Systems Operator (NPSO, later Pay.UK) strategies which were only released in 2016. More specifically, the analytical model delivered in **[3.2]**, branded under the concept 'Collective Intelligence Hub' (CIH) *"was seen at the time to offer a realistic and usable approach to how data sharing for counter-fraud purposes in the public sector (e.g. for Universal Credit) could be automated to provide additional protection for public money."* **[5.2]** and was presented in

December 2014 to a panel of financial services executives and payments industry stakeholders, coordinated by CIFAS (Credit Industry Fraud Avoidance Scheme) and advising the Government Coordination Committee, as outlined in (2) below. While the proposal was not adopted at the time, the Collective Intelligence Hub was later presented in the form of a technological framework and solution in March 2016 to the Payments Strategy Forum (PSF; established Feb 2015), at the early stages of deliberations in the Financial Crime Data and Security Working Group, whose *"remit was to identify initiatives, where the industry could collaborate and work with Government, to deliver step-change capabilities to tackle fraud and financial crime risk in payments"* **[5.3]**. The CIH proposal was formally recognised to be commensurate with the strategic vision of the PSF.

The underpinning work has addressed solutions applicable in both public and private sectors; the academic research, outlined in Section 2, concentrated on the use of AI approaches for combatting fraud in electronic payments networks and on developing Anti-Money Laundering models and solutions. Throughout the impact period (2012-2020), the research contributed directly on the recommendation of appropriate tools, techniques and infrastructure for future deployment, in both the UK financial services and public sector. In the impact period, the contribution trajectory took the form outlined here:

1) The underpinning research has attracted attention in the commerce field, and led to invited disseminations of research propositions in industry conferences and sector discussion panels. These events **[5.5 - 5.9]** thematically focused on operational and economic significance of intelligent techniques against fraud and money laundering. The resulting visibility of underpinning research attracted further attention by stakeholders in public policy (DWP) and regulation (FCA, CIFAS), subsequently leading to his direct involvement in activities outlined in (2), (3) and (4) immediately below.

2) On 17 December 2014, **Samakovitis'** proposal for a UK-wide data sharing collaborative model was formally presented to a panel of banking professionals, (including representatives of the Bank of England and Financial Fraud Action (FFA UK)) advising the UK Government Coordination Committee. Termed Collective Intelligence Hub (CIH), the proposed model was "*one of the very few approaches at the time that suggested leveraging anonymous transaction data sharing between financial institutions*" **[5.2]**, as discussed later in this section. Although the legal challenges associated with such data sharing, both in the public and private sectors were such as to prevent practical actions being taken at the time, the "*CIH approach added value by making explicit the potential benefits that could be realised if financial institutions could find a way to share data in order to counter money laundering and fraud, through **[**the CIH**]** specific model for doing so*" **[5.2]**. This involvement further motivated his recommended introduction to the then newly-founded Payments Strategy Forum (PSF).

3) From April 2015 (and until the completion of its objectives in December 2017) **Samakovitis** was a member and direct participant of the UK Payments Strategy Forum (PSF), a body commissioned by the new Payment Systems Regulator (https://www.psr.org.uk/about-psr) as the main industry and policy forum on the UK's future payments strategy for the next 20 years (https://www.psr.org.uk/developing-payments-strategy-forum). Throughout that period (2015-17) "*the contributions by Dr. Samakovitis had continued presence and hence materially influenced the direction of the Working Group, particularly with reference to infrastructure and governance for anti-money laundering data sharing and utilisation"* **[5.3]**. His distinct material contribution concentrated on the outputs of the Financial Crime Data and Security Working Group (https://consultation.paymentsforum.uk/workinggroups/financial-crime), primarily under two Strategic Solutions: (i) **Trusted KYC Data Sharing**; a solution framework for a central shared repository to support financial services providers in their Know-Your-Customer (KYC) procedures and; (ii) **Payments Transaction Data Sharing & Data Analytics;** a solution framework that involves a centralised transaction storage facility and analytical capability, residing with a public body. Both solutions formed part of PSF's "*recommended development of a transaction data analytics capability to be built for Faster Payments and BACS, the UK's retail payments market infrastructure..[..]..Subsequent to the Forum's work, this solution was implemented for Faster Payments in 2018, called MITS (Mule Insights Tactical Solution), and will be incorporated and enhanced in the new NPA* [New Payments Architecture] *infrastructure"* **[5.3]**. In both Strategic Solution spaces, the operational principles and technological architecture proposed by **Samakovitis** were "*recognised as* *commensurate with the strategic vision of the PSF, and considered as supporting elements of the solutions that the Working Group later submitted to the Payment Systems Regulator"* **[5.3]**.

Collaboration with UK Government stakeholders and PSF Working Group participants has catalysed **Dr. Samakovitis'** direct membership in the Counter Fraud Data Analytics Advisory Group of the HMG Cabinet Office (Counter Fraud Centre of Expertise), *"..an established group of industry leaders, academics and third sector representative, …[which]…provides a forum for ongoing consultation, challenge and support for the development of the Profession"* (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/730050/Annex_B_-_GCFP_Brochure.pdf). Within the remit of the Advisory Group, "*his underpinning research contribution has directly and materially supported clearer understanding of the technological solution space for identifying and mitigating fraud in the public sector"* **[5.4]**. Along the same lines, the insights grounded on **Dr. Samakovitis'** underpinning research *"have had distinct and material contribution to informing the Counter Fraud Data Analytics Standard and, in so doing, supporting the establishment of role and education specifications for the Counter Fraud Profession in Government*" **[5.4]**. In his capacity as academic advisor, he has directly supported the Cabinet Office Ministerial Thought Paper on fraud in the government sector **[5.1]** through a named contribution (pp. 64-67) proposing four core themes along which Government should pursue data sharing strategies. According to the Programme Director, Counter Fraud Centre of Expertise, "*research input by Dr. Samakovitis, introduced via his participation in the Advisory Group has materially informed and, to an extent, influenced the Centre's position on how data sharing strategies can improve Civil Service operation, and contributes to its work in shaping the direction of the Counter Fraud function in Government"* **[5.4]**

5. Sources to corroborate the impact

Evidence of the impacts:

1. HMG Cabinet Office Thought Paper (2019): Tackling Fraud in Government with Data Analytics: Starting the Conversation, Department for Digital, Culture, Media & Sports, June 2019 (pp. 64-67), https://www.gov.uk/government/publications/tackling-fraud-in-government-with-data-analytics

2. Testimonial – Innovation Lead, CDIO, HMRC, UK.

3. Testimonial – Former Payments Strategy Forum Working Group Programme Lead, UK

4. Testimonial – Programme Director, Counter Fraud Centre of Expertise, Cabinet Office, UK.

Evidence of the impact translation activities (media interviews; trade conference presentations; industry events):

5. 'AI and advanced analytics in AML: From rule-based controls to intelligence-led capabilities' Interview by C. de Monts-Petit, Editor, The Economist Intelligence Unit, Feb. 2020, available at: https://eiuperspectives.economist.com/technology-innovation/ai-and-advanced-analytics-aml-rule-based-controls-intelligence-led-capabilities

6. Samakovitis, G. (2018), 'RegTech and the Role of Artificial Intelligence' Invited Panel Session MLROs London Conference Three, London, 26 Sep 2018

7. Samakovitis, G. (2017), 'Collective Intelligence for Client Onboarding: What AI can do for you (and what it cannot)', Client Onboarding in Financial Services (22-23 Feb 2017),

8. Samakovitis, G. (2016), 'Towards Collective Intelligence for AML: an Operational & Technological Framework for Addressing the Risk Balance across the Value Transfer Ecosystem', Client Onboarding in Financial Services (24-25 Feb 2016),

9. Samakovitis, G. (2014), 'Financial Transactions Monitoring & Fraud Detection – Challenges in the Current Environment', Info Crime: Information Security and Cyber Crime Summit (18-19 Feb 2014).