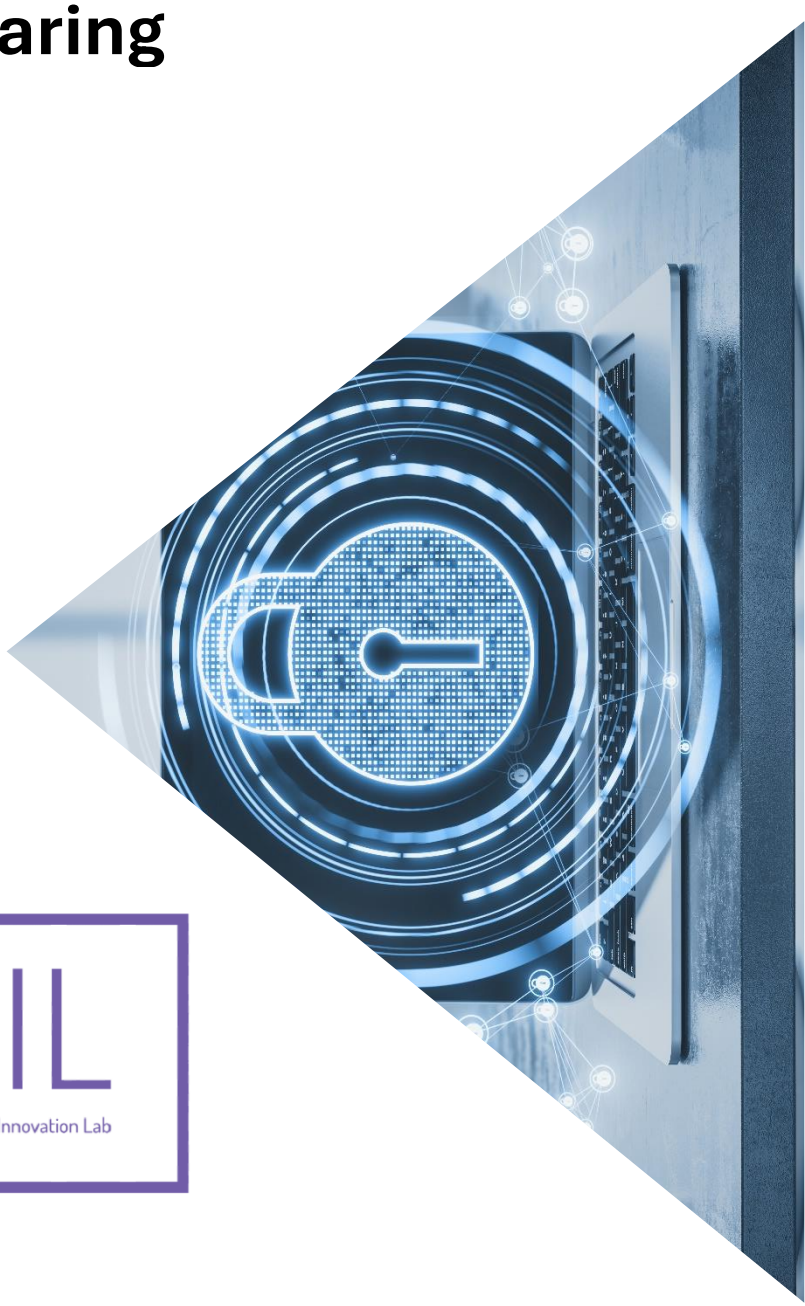
ISSN: 3033-4136

DOI: https://doi.org/10.17868/strath.00092425

Authorised Push Payment Fraud Mitigation: The Role of Data and Information Sharing



FRIL
Financial Regulation Innovation Lab

FinTech Scotland®

University of Glasgow

University of Strathclyde Glasgow

Devraj Basu, Strathclyde Business School, University of Strathclyde

We acknowledge funding from Innovate UK, award number 10055559.

Many thanks to Zonathan Hass and Daniel Turner-Szymkiewicz for their inputs and insights, particularly around the components of an APP Fraud Library for comments on earlier drafts.

Corresponding author:
Email: devraj.basu@strath.ac.uk;

Open Access. Some rights reserved.
Open Access. Some rights reserved. The publishers, the University of Strathclyde and FinTech Scotland, and the authors, Devraj Basu wants to encourage the circulation of his work as widely as possible while retaining the copyright. We therefore have an open access policy which enables anyone to access our content online without charge. Anyone can download, save, perform or distribute this work in any format, including translation, without written permission. This is subject to the terms of the Creative Commons by ShareAlike licence. The main conditions are:

- The University of Glasgow, FinTech Scotland, and the authors are credited, including our web addresses **www.strath.ac.uk** and **www.fintechscotland.com**
- If you use our work, you share the results under a similar licence

A full copy of the licence can be found at
https://creativecommons.org/licenses/by/4.0/
You are welcome to ask for permission to use this work for purposes other than those covered by the licence.

We gratefully acknowledge the work of Creative Commons in inspiring our approach to copyright. To find out more go to **www.creativecommons.org**

Financial Regulation Innovation Lab

Who are we?

The Financial Regulation Innovation Lab (FRIL) is an industry-led collaborative research and innovation programme focused on leveraging new technologies to respond to, shape, and help evolve the future regulatory landscape in the UK and globally, helping to create new employment and business opportunities, and enabling the future talent.

FRIL provides an environment for participants to engage and collaborate on the dynamic demands of financial regulation, explore, test and experiment with new technologies, build confidence in solutions and demonstrate their ability to meet regulatory standards worldwide.

What is Actionable Research?

FRIL will integrate academic research with an industry relevant agenda, focused on enabling knowledge on cutting-edge topics such as generative and explainable AI, advanced analytics, advanced computing, and earth-intelligent data as applied to financial regulation. The approach fosters cross sector learning to produce a series of papers, actionable recommendations and strategic plans that can be tested in the innovation environment, in collaboration across industry and regulators.

Locally-led Innovation Accelerators delivered in partnership with DSIT, Innovate UK and City Regions

Department for Science, Innovation & Technology

UKRI Innovate UK

GLASGOW CITY REGION

FRIL White Paper Series

Authorised Push Payment Fraud Mitigation: The Role of Data and Information Sharing

Devraj Basu

** University of Strathclyde*

February 2025

Abstract: Authorised Push Payment (APP) fraud has been increasingly steadily, with many of the common types originating on social media and the internet. Combatting and mitigating APP fraud will require cooperation across financial institutions and tech and telecoms companies, with data and information sharing playing a key role. Recent UK legislation aims to facilitate data and information sharing to combat fraud and privacy enhancing technologies (PETs) provide technical solutions to enable better understanding and widespread sharing of fraud intelligence that enable data protection and privacy.

Contents

1. Introduction 6
2. Data Sharing: The UK Legal Framework 7
3. APP Fraud Types 8
4. Synthetic Data and Privacy Enhancing Technologies (PETs) 8
5. Conclusion 11
6. Appendix: Components of an APP Fraud Library 11
    1. Perpetrator Characteristics: 11
    2. Perpetrator Transaction Behaviours: 11
    3. Victim Characteristics: 12
    4. Victim Behavioural Patterns: 12
    5. General Framework and Statistical Distributions: 12
About the Author 13

1. Introduction

Cases of authorised push payment (APP) scams in the UK, where victims are tricked into sending money to fraudsters, rose by 12 per cent in 2023 to about 230,000 cases, fuelled by a 36 per cent increase in purchase scams, where criminals sell goods, such as concert tickets, which never materialise. Such scams made up nearly 70 per cent of all APP fraud and accounted for a record £86m in losses. Romance scams, another type of APP fraud, where people are beguiled into sending money to someone, they believe they are in a relationship with, also reached record highs in terms of amounts lost and number of cases. Criminals stole a total of £36.5m last year posing as romantic partners, 17 per cent more than the previous year. Despite the rise in cases, the amounts lost to APP fraud fell by 5 per cent last year to £459.7m, while financial institutions such as banks and payment companies did a better job at reimbursing victims.

Reimbursement has jumped from 61 percent of money lost in 2022 to 67 percent in 2023, with some banks returning lost funds in full more than 90 percent of the time. There is a wide variance across banks in percent of cases fully refunded, with Nationwide, TSB and Barclays refunding customers in full 96, 95 and 82 percent of time while Monzo, Danske Bank and AIB refunded customers in full less than 10 percent of the time. In this context, the categorisation of a fraud event as an APP fraud depends on the individual bank. It has been noted that banks do not consider cryptocurrency investment fraud as APP fraud and sometimes classify APP frauds as civil disputes[1]. The Payment Services Regulator (PSR) has published a consultation draft guidance on supporting the identification of APP scams and civil disputes[2] which outline factors that payment services providers should consider when identifying whether a claim relates to a civil dispute or a reimbursable APP scam. Initial responses suggest that there appears to be a lack of focus on payments made for goods and services advertised via online peer-to-peer marketplaces such as Facebook Marketplace where much of the fraud seems to originate, as well as a lack of guidance around what constitutes a civil dispute and a genuine APP scam[3].

New measures which started in October 2024 from the Payments Service Regulator require banks and other payment providers to reimburse victims of APP fraud up to a limit of £85,000. The reimbursement cost would be split between the financial institutions used to send and receive the payment, with the sending firm required to notify the receiving firm of the scam within two hours. The proposals come under new powers given to the PSR under the UK Government's Financial Services and Markets Act (2023), which came into force in June 2023. The significant role tech companies can play in combatting APP fraud has been highlighted with more than 70 percent of APP fraud originating online. The current UK Labour Government has drafted plans to make tech companies liable to reimburse victims, outlining a proposal where banks would still have the obligation to refund fraud victims but could in turn claim a settlement compensation back from tech companies. Bank and payment companies would regularly submit evidence to an

---

1 https://www.linkedin.com/feed/update/urn:li:activity:7224729477740707840/

2 https://www.psr.org.uk/publications/consultations/cp2410-consultation-on-draft-guidance-on-supporting-the-identification-of-app-scams-and-civil-disputes/

3 https://www.innovatefinance.com/consultation/psr-consultation-cp24-10-draft-guidance-on-supporting-the-identification-of-app-scams-and-civil-disputes-innovate-finance-response/

oversight body, which would then determine how much tech companies should contribute.

2. Data Sharing: The UK Legal Framework

The initiation of data sharing across banks, tech companies and law enforcement could be an effective way of preventing and mitigating APP fraud. Currently all these entities operate in siloes and are unable to completely understand how sophisticated organised crime groups, who trade intelligence on the best way to target consumers, carry out their operations. The UK Economic Crime and Corporate Transparency Act 2023 (ECCTA)[4] makes information sharing easier. Under the Act, a firm can share information with another firm for the purposes of preventing, detecting, and investigating economic crime, without involvement from law enforcement or a request from the recipient firm. So long as certain conditions are met, the sharing and recipient firms are protected from certain civil claims by the relevant customer or any other party. There are two options, direct sharing, or indirect sharing via a third-party intermediary. A firm is however only free to volunteer information about a customer proactively when it has committed to taking safeguarding action against that customer themselves (or would have done if they were still a customer). A firm may wish to share information about a customer that is relevant to preventing, detecting, or investigating economic crime, but it may not be possible to identify another firm to which that information would be useful. For example, where a bank exits a customer relationship due to economic crime concerns, it will not necessarily be able to identify any banks to which the customer will apply in the future. In its Impact Assessment[5], the government did not specify how the proposed third-party sharing platform is to operate observing: "Whilst the measure does not mandate information sharing between firms, nor specify the mechanism via which sharing must take place, the most likely scenario to arise following introduction of the measure (based on extensive feedback and engagement with the financial sector) is a privately funded third party platform for exchanging information on economic crime, similar to the Cifas hosted National Fraud Database".

A voluntary data sharing deal among seven banks to share customer data with the National Crime Agency (NCA) in the largest project of its kind worldwide to tackle criminal gangs, money laundering and "dirty money" flowing through the country has been ongoing since May 2024[6]. Under the programme that is due to run until October 2024, bank staff are seconded to the NCA to form a team of between 15 to 20 intelligence officers, data scientists and analysts to probe movement of money suggestive of criminal behaviour - and ensure legitimate customers are left alone. Only data with multiple clear indicators of financial crime is shared which goes some way towards addressing data privacy issues. Singapore launched COSMIC[7] with six banks, a digital platform that allows secure sharing of information on customers who share multiple "red flags" that may indicate potential financial crime concerns, if stipulated thresholds are met.

[4] https://www.legislation.gov.uk/ukpga/2023/56

[5] https://assets.publishing.service.gov.uk/media/63d270a3e90e071ba44851f9/_f__Information_Sharing_IA_Jan_2023_-_signed.pdf

[6] Seven banks share data with UK law enforcement in 'dirty money' crackdown | Reuters

[7] https://www.mas.gov.sg/regulation/anti-money-laundering/cosmic

3. APP Fraud Types

In the context of APP fraud there are eight major categories that can be identified, based on a classification done by the trade body UK Finance. These are:

1. Purchase Scam: In this type of fraud, scammers pose as legitimate sellers and convince victims to pay for goods or services that are never provided.

2. Investment Scam: Fraudsters persuade victims to invest in fictitious schemes, often promising high returns.

3. Romance Scam: Scammers create fake online profiles to exploit the emotions of their victims and request money under false pretences. This can cause both financial and emotional distress for the victim.

4. Advance Fee Scam: Victims are tricked into paying an upfront fee with the promise of receiving a larger sum or valuable goods later. This can lead to financial loss and a feeling of being deceived.

5. Invoice and Mandate Scam: By manipulating invoices, scammers trick victims into redirecting payments to fraudulent accounts. This can cause financial harm to both individuals and businesses.

6. CEO Scam: Fraudsters impersonate high-ranking officials and pressure employees into making urgent payments to controlled accounts. This scam primarily targets businesses.

7. Impersonation Scam: Police/Bank Staff Scam: Criminals pose as law enforcement or bank staff and coerce victims into transferring money to 'safe accounts'.

8. Impersonation Scam: Other: Scammers impersonate representatives of various organisations and create scenarios to pressure victims into making payments.

All these fraud types could potentially involve several institutions, both financial as well as tech, so that secure information sharing would be very helpful in this context. UK Finance analysis of nearly seven thousand authorised push payment (APP) scam cases shows that more than 70 per cent of scams originated on an online platform, with most investment (96 per cent), romance (96 per cent) and nearly all purchase (98 per cent) scams originated online, highlighting the internet's significant role in enabling fraud[8]. Provisions 188 and 189 of the ECCTA disapply civil liability for breach of confidentiality for regulated sector businesses sharing information in specific circumstances. This removes one of the key perceived barriers to information-sharing on economic crime in the regulated sector. In doing so, the act provides legal certainty for banks and wider regulated sectors to share financial crime information, both peer-to-peer and via a third-party platform. The protections and appeals mechanism outlined in the Act will be based on the Cifas National Fraud Database.

4. Synthetic Data and Privacy Enhancing Technologies (PETs)

However, several issues around data and information sharing remain, either directly or via a third-party platform. A major concern is privacy and data protection as the data and information pertain to individuals and constitute personally identifiable information (PII). The businesses' existing obligations under data protection regulations such as GDPR remain. In this context data technology presents opportunities to facilitate information sharing in the context of financial

[8] https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online-new-uk-finance-analysis

crime, with the key technologies being classed as Privacy Enhancing Technologies.

The term Privacy Enhancing Technologies (PETs) captures a range of tools and techniques, each with a distinct set of analytical capabilities (and a distinct set of limitations). Broadly speaking, PETs are a set of emergent technologies and techniques that help to operationalize fundamental data protection principles by minimizing personal data use, transforming data in privacy-preserving ways, and/or maximizing data integrity, confidentiality, and security. When applied appropriately, PETs can help meet data protection requirements while unlocking data utility. The European Union Agency for Cybersecurity (ENISA) refers to PETs as: Software and hardware solutions, ie systems encompassing technical processes, methods or knowledge to achieve specific privacy or data protection functionality or to protect against risks of privacy of an individual or a group of natural persons

There are broadly seven major techniques:

1)Differential privacy, where noise is added to an analytical system so that it is impossible to reverse-engineer the individual inputs.

2)Federated analysis, where parties share the insights from their analysis without sharing the data itself.

3) Homomorphic encryption, where data is encrypted before it is shared, such that it can still be analysed but not decoded into the original information. Homomorphic encryption enables complex mathematical operations to be performed on encrypted data without compromising the encryption.

4)Zero-knowledge proofs, where users can prove their knowledge of a value without revealing the value itself.

5)Secure multiparty computation, where data analysis is spread across multiple parties such that no individual party can see the complete set of inputs.

6) Trusted Execution Environment (TEEs) which is a processing environment isolated from a computer's main processor and memory. TEEs provide a signed description of the code that will be run, called an attestation. The parties can check the attestation, and once they're comfortable, they will share the data and the computation is performed.

7) Synthetic data generates data sets that are non-identifiable so that these can be used and disclosed without the legislative need for additional consent as these data sets would not be considered personal information.

Differential privacy allows sharing of an output that is similar to the data, rather than the data itself. It is designed to limit the ability of an outsider to identify information about specific individuals while sharing useful insights about a group or the data set as a whole. Federated learning is a PET that allows the building of shared tools without ever sharing the underlying data used to train those tools. It could be informally described as "models going to the data, rather than data going to the models". Google currently uses federated learning to train the speech models that power its "Google Assistant" offering without ever moving audio data to Google's central servers. The other four techniques all allow for deriving specific pieces of information or insights from a dataset without seeing all the underlying data. In the context of economic crime, the Homomorphic Encryption Applications and Technology project had a use case that enabled data sharing for organized crime detection between EU countries while respecting the strong EU legal constraints on privacy[9].

PETs can help demonstrate a data protection by design and default approach as in Article 25 of GDPR. Data protection by design means

[9] http://www.goubin.fr/papers/Barnett_etal.pdf

embedding data privacy features and data privacy enhancing technologies directly into the design of projects at an early stage. This will help to ensure better and more cost-effective protection for individual data privacy. Data protection by default means that the user service settings (e.g. no automatic opt-ins on customer account pages) must be automatically data protection friendly, and that only data which is necessary for each specific purpose of the processing should be gathered at all. In the UK the Information Commissioner's Office (ICO) has provided guidance around PETs aimed at Data Protection Officers and others using large personal data sets in finance, healthcare, research, and central and local government[10]. A PETs based start-up ecosystem is starting to develop in the UK with Regulaition focused on federated learning, differential privacy and multi-party computation and Verifoxx focusing on zero-knowledge proofs, homomorphic encryption and trusted execution environments, while the financial crime focused start-up Featurespace have developed privacy preserving solutions for financial crime detection using local differential privacy which won awards at the UK-US PETs challenge[11].

In the context of APP fraud where much of the initial fraud originates online, the telecommunications companies hold much of the relevant data from which fraud indicators can be identified. A coalition of the UK's largest banks and telecoms companies led by Which?, including Barclays, BT, Mobile UK, Nationwide, NatWest, Starling, Three UK, UK Finance, Virgin Media O2 and Vodafone, have called on the UK Government to lead the taskforce to share APP fraud data which must work across industry sectors , and deliver technical solutions to generate a data application that can be used to prevent fraud across UK digital channels[12]. The legal framework would follow from the ECCTA and the PETs outlined above could enable the necessary technical solutions. The GSMA, which unites over 1000 mobile operators and businesses across the ecosystem, is looking into how telecoms companies could share data with banks via PETs to stop fraud and have had discussions in this regard with Verifoxx, who are working with the Financial Conduct Authority on a PETs based solution for information sharing to combat APP fraud. There is substantial interest around PETs based solutions that could enable banks and telcos to share information around APP fraud.

A synthetic data library of common APP fraud types as outlined in the previous section would enable financial institutions to mitigate their APP fraud risks in several ways. A detailed library of APP fraud typologies would help financial institutions identify vulnerabilities in their existing fraud controls and compare their control performance against industry peers. This library would provide institutions with a better understanding of the risk profile of various fraud types and estimate potential losses from various APP fraud types, thus helping institutions understand the magnitude of the threat and prioritize their efforts accordingly. The typology library would facilitate seamless cross-institutional cooperation by offering a standardised framework that fosters sharing of critical information on emerging threats and best practices. Moreover, it assists in aligning prevention strategies with international norms, thereby enhancing the capacity of financial institutions to operate effectively and harmoniously on a global scale, united in their front against financial crimes. Using the insights gained from the simulations and benchmarking, institutions can tune their controls to enhance performance with

[10] https://ico.org.uk/media/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies-1-0.pdf

[11] https://petsprizechallenges.com/

[12] https://www.techdigest.tv/2024/08/which-led-consortium-urges-government-to-make-fraud-priority-by-removing-barriers-to-data-sharing.html

continuous improvement of fraud controls ensuring that institutions remain a step ahead of evolving fraud tactics. These improvements could be driven by leveraging the power of AI and machine learning to analyse anomalies in financial transactions allowing institutions to build high-performance AI defences. An example of such an APP fraud library is the Synthesizor platform built by Fincrime Dynamics [13]. Synthetic data solutions have been developed for financial crime beginning with the PaySim[14] data set with the largest project being the synthetic data set developed in the Bank of International Settlement's Project Hertha[15].

5. Conclusion

Authorised Push Payment (APP) fraud has grown rapidly in the last few years and several legal and regulatory remedies are being put in place to combat it. Data and intelligence sharing could be a key tool in fighting APP fraud with a legal framework emerging in the UK to make it possible. Privacy enhancing technologies (PETs) are a suite of technologies that could provide the necessary data protection to enable better understanding and widespread sharing of fraud intelligence.

References

Payment Systems Regulator (2024), *Authorized Push Payment (APP) scams performance report,* July 2024, 1-37 available at https://www.psr.org.uk/information-for-consumers/app-fraud-performance-data/

Payment Services Regulator (2024), *Policy Statement: Faster Payments APP Scam Reimbursement Requirement,* October 2024, 1-31 available at https://www.psr.org.uk/media/e30pwlly/ps24-7-app-scams-maximum-level-of-reimbursement-policy-statement-oct-2024.pdf

6. Appendix: Components of an APP Fraud Library

This appendix is based on the methodology used by Fincrime Dynamics [16] .

The main components for a simulation are amount, time series and patterns/behaviours. With that in mind, for fraud typologies we concentrate on a few macros such as:

Transaction amount - Velocity –monitoring frequency and pattern of transactions made within a specific time frame

Seasonality -

Research points - primary, secondary, tertiary

1. Perpetrator Characteristics:

- Number of Criminal Accounts: Total number of perpetrators involved.
- Demographics: Characteristics such as age, gender, etc., for continuous and categorical data.
- Probability of Money from Internal/External Sources: Probability of perpetrators getting money from internal or external accounts.
- Maximum Scam Amount: Limit on the amount involved in scams.

2. Perpetrator Transaction Behaviours:

- Inflow Amount Distribution: Patterns of scam amounts received.
- Number of Outflow Accounts Distribution: Distribution for the number of accounts perpetrators transfer money to.

[13] Appendix A outlines potential components of such an APP Fraud Library

[14] https://github.com/EdgarLopezPhD/PaySim

[15] https://www.bis.org/about/bisih/topics/fmis/hertha.htm

[16] See https://thepaymentsassociation.org/article/addressing-app-fraud-introducing-fincrime-dynamics-app-fraud-testing/ for more information.

- Outflow Velocity Distribution: Rate of transferring money out.
- Inflow Round Figure Probability: Likelihood of scam amounts being round figures.
- Transactional Activity Distribution: Typical hours of the day when transactions occur.
- Scam Hours Discrete Distribution: Specific time slots indicating higher scam activity.

3. Victim Characteristics:

- Number of Victims: Total count of scam victims.
- Demographics: Victim demographic data for continuous and categorical data.
- Internal Perpetrator Probability: Likelihood of being scammed by an internal perpetrator.
- Maximum Scam Amount: Upper limit on scam amounts faced by victims.

4. Victim Behavioural Patterns:

- Scam Amount Distribution: Patterns of scam amounts faced by victims.
- Period Until Perception Distribution: Time taken by victims to detect a scam.
- Number of Outflow Accounts Distribution: Distribution for the number of accounts to which victims transfer money.
- Round Figure Probability: Chance of scam amounts being in round figures.
- Relapse Probability Distribution: Likelihood of victims facing repeated scams.
- In Between Scam Behaviour: Behavioural patterns of victims between scams.
- Transactional Behaviour Prior to Scam: Behavioural patterns before falling victim to scams.
- Periodicity of Scam: Frequency at which victims encounter scams.

5. General Framework and Statistical Distributions:

- Effectiveness Start and End: Time frame for the start and end of scam effectiveness.
- Effectiveness Distribution: Distribution of the total number of scams over a period.
- Continuous Distributions: Including Exponential, Normal/Gaussian, Gamma, Beta, Uniform.
- Discrete Distributions: Including Poisson, Bernoulli, Hypergeometric.
- Categorical Distributions: Probability-based distribution for various categories

.

About the Author

Dr. Devraj Basu is Senior Lecturer in Finance in the Accounting and Finance department at Strathclyde Business School. His area of academic research is financial markets, covering equity markets, commodity markets and alternative investments, as well as quantitative finance. He has published in top ranked international peer reviewed journals as well as top industry journals. He is actively involved in Regtech having set up the Regtech Forum which bring together industry, academia and government both within Scotland and internationally. The goal of the Regtech Forum is to help understand the fast moving Regtech landscape and how Scotland and the UK can position themselves to become leading global players. He has helped design Strathclyde's MSc in Financial Technology, the UK's first master's program in Fintech.

Email: devraj.basu@strath.ac.uk

Get in touch

FRIL@FinTechscotland.com

This is subject to the terms of the
Creative Commons license.
A full copy of the license can be found at
https://creativecommons.org/licenses/by/4.0/

FinTech Scotland®

University of Glasgow

University of Strathclyde Glasgow