

The Role of Technology & Public Private Partnerships in Fighting Financial Crime

Professor Daniel Broby Chair of Financial Technology, Ulster University

Inspector Steven Meighan BL Garda National Economic Crime Bureau (GNECB), FIU Ireland

Andrew Quinn Director, PAT Fintech

CPD CODE: 2022-0012



Welcome & Introduction



- Thank you for registering
- Questions
 - Please use the question box on the right of your screen to send the questions for our speaker
- Today's session will be recorded and will be on our website later today
- The CPD code is noted below and will be sent out directly after this session has concluded

CPD CODE: 2022-0012

Upcoming Webinars



WEBINAR
Data Breaches and Data Subject Access Requests
27 January | 1:00pm

Chris Bolland
A&L Goodbody

Andrea Lawler
A&L Goodbody

compliance.ie

WEBINAR
World Data Protection Day
28 January | 1:00pm

Speaker:
Garrett O'Neill
Assistant Commissioner Data Protection Office

compliance.ie

WEBINAR
Doing the Right Thing: Embedding Business Ethics
9 February | TBC

Catherine Vaughan
EY

compliance.ie

WEBINAR
Central Bank of Ireland: Speaking Engagement
21 February | TBC

Speaker:
Gerry Cross
Central Bank of Ireland

compliance.ie

Data Breaches & Data Subject Access Requests

27th January @ 1pm

1 Hour LCOI, FCOI (Compliance), CDPO

World Data Protection Day – FREE EVENT

28th January @ 1pm

1 Hour LCOI, FCOI (Compliance), CDPO

Doing the Right Thing: Embedding Business Ethics – FREE FOR MEMBERS

9th February @ 1pm

CPD TBC

Central Bank of Ireland: Speaking Engagement – FREE FOR MEMBERS

21st February @ 1pm

CPD TBC

Panel



Professor Daniel Broby Chair of Financial
Technology, Ulster University



Inspector Steven Meighan BL Garda
National Economic Crime Bureau
(GNECB), FIU Ireland



Andrew Quinn Director, PAT Fintech

Attendee Takeaway's



Demonstrate how technologically enhanced monitoring systems, and data sharing, can fundamentally improve the quality of suspicious transaction alerts.

Develop their practical understanding of how technology can both reduce the costs and the level of operational risk within the financial services industry.

Reference tangible examples of the role of Public Private Partnerships in fighting Financial Crime.

Analyse the critical components of the 'data issue' in building effective Public Private Partnerships (PPPs).

The Role of Technology in Fighting Financial Crime

Professor Daniel Broby Chair of Financial
Technology, Ulster University

CPD CODE: 2022-0012



Regulatory technology (regtech)

- Regtech” is a term used to describe how different stakeholders use digital technology to enforce, oversee and implement legal and regulatory rules.
- Regtech can be used to enhance regulatory outcomes and assist with corporate governance and oversight.
- Regtech to date has focused on the digitization of manual reporting and compliance processes, for example in the context of know-your-customer requirements.
- This offers tremendous cost savings to the financial services industry and regulators.
- Regtech could enable a real-time and proportionate regulatory regime that identifies and addresses risk while also facilitating more efficient regulatory compliance.

Compliance oversight

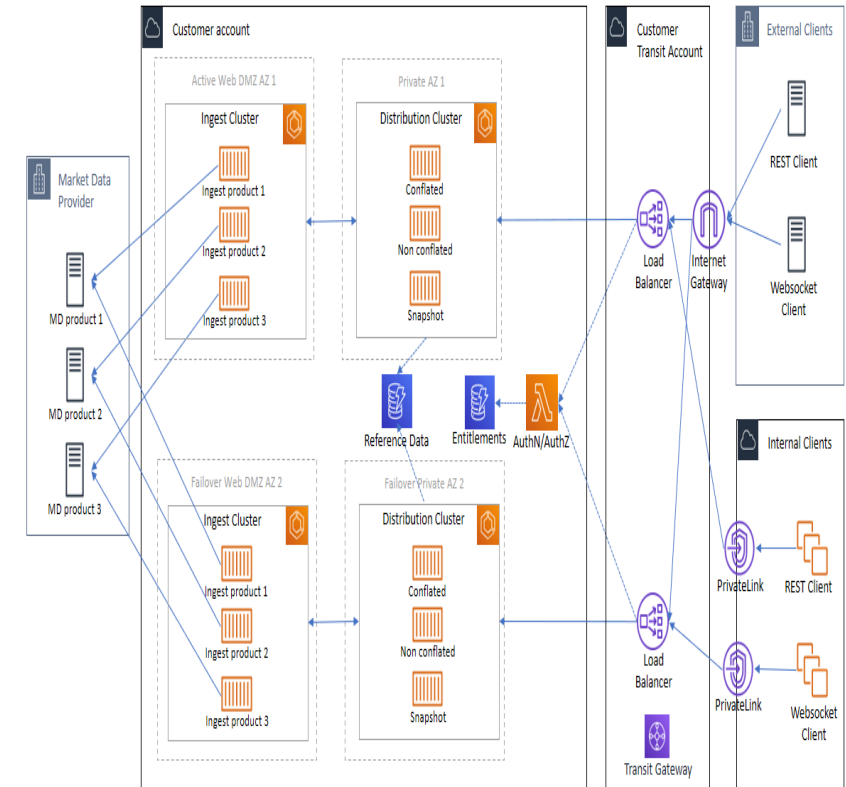


- Compliance should provide an extra set of eyes to verify that the firm understands both its and its customers risk profile and is sufficiently capitalized against the risks.
- Credit risk is economic loss that emanates from the failure of a counterparty to fulfil its contractual obligations (e.g., timely payment of interest or principal), or from the increased risk of default during the term of the transaction.
- Market risk is the risk that emanates from investing, trading, and generally from having exposure to financial markets.
- Operational risk management entails the firm seeking to identify the risk of direct or indirect financial loss emanating from a host of potential operational breakdowns.

Digital compliance



- We are in a digital revolution - that is well documented.
- As part of that, financial services have generated an explosion in data.
- The processing of this data requires a range of skills that are not traditional associated with compliance and oversight.
- These include Computer Programming Languages, Data Base Management, Artificial Intelligence, Machine Learning, Pattern Recognition and Visualization.
- Regulatory Technology (RegTech) increases efficiency and has the ability to take complex, manual processes and streamline them.



Source: AWS.

Decision Support System techniques

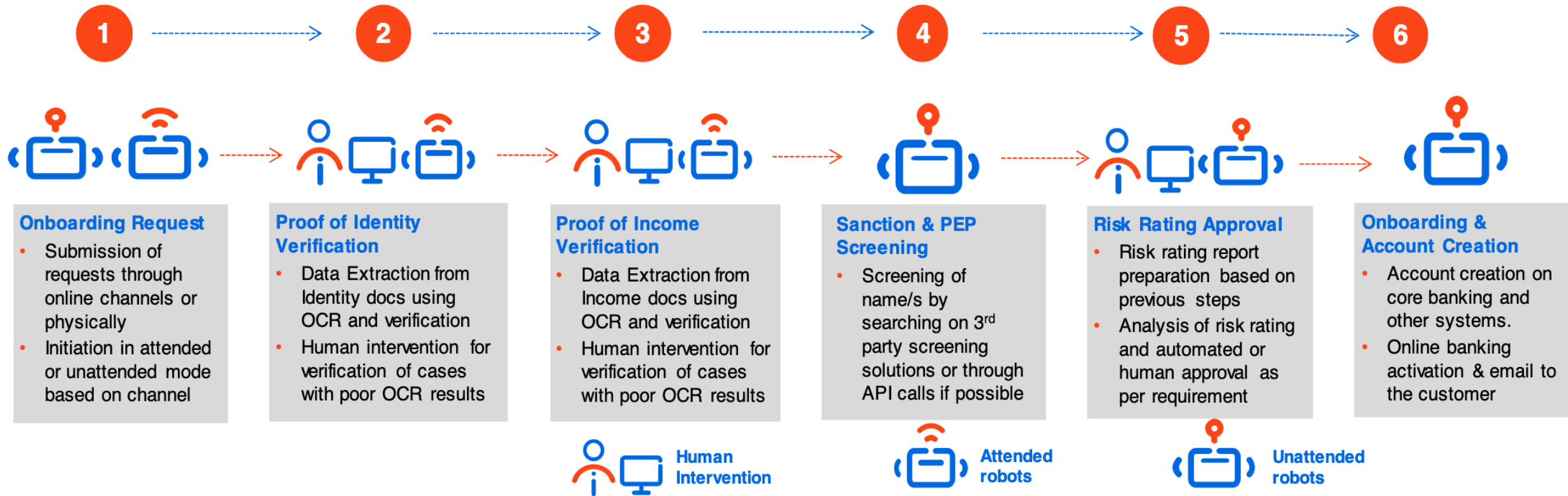


- Regression (or prediction) — a task of predicting the next value based on the previous values.
- Classification — a task of separating things into different categories.
- Clustering — similar to classification but the classes are unknown, grouping things by their similarity.
- Association rule learning (or recommendation) — a task of recommending something based on the previous experience.
- Dimensionality reduction — or generalization, a task of searching common and most important features in multiple examples.
- Generative models — a task of creating something based on the previous knowledge of the distribution.

Detecting fraud

- Big data analysis can help detect fraud in a preventative way (Bhattacharyya, Jha, Tharakunnel, and Westland (2011))
- Credit card fraud is typically only identified with a time lag. The perpetrators therefore have time in which to commit multiple offences with the same account.
- Perols, Bowen, Zimmermann, and Samba (2017) point out that prediction is made difficult due to the rarity of fraud, the large numbers of explanatory variables and the large number of different types of fraud.
- Ngai, Hu, Wong, Chen, and Sun (2011) provide a classification and literature review on the latter. It is clear from their work, and the work of other scholars, that successful frauds are complex and hard to detect.
- For example, fraudulent activity at Madoff Investment Securities LLC was documented for ten years prior to being exposed by a fund manager who mathematically should the performance track record was mathematically impossible to achieve.

Robotics

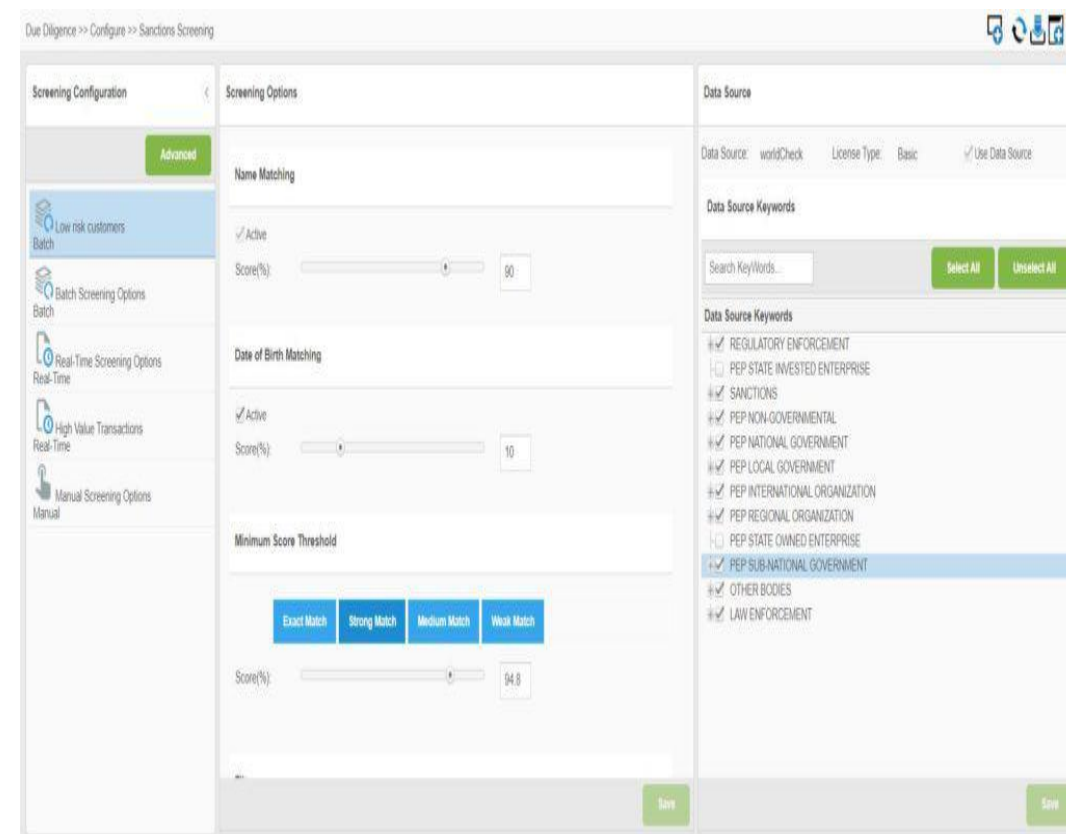


Source: MEDICI Global

Technologically enhanced monitoring systems



- Name check and identified aliases.
- Negative media.
- Global compliance checks.
- Corporate filings.
- Individual business interest checks.
- Litigation checks
- Bankruptcy checks
- Regulatory checks
- Executive risk summary and analysis
- Ultimate beneficial owner (UBO) – identification of all physical persons holding a significant percentage of the company's shares



Source: Alessa. A tool that has different screening parameters for entities, individuals and transactions

Identify management

- In a data driven financial system, everyone leaves a financial digital footprint.
- An important area in identity management and control is the focus on counterpart due diligence, Know Your Client (KYC) procedures, anti-money laundering (AML) controls and fraud detection.
 - For instance, digitalization of client or partner onboarding processes, digitization and sharing of customer/partner information, gathering and analyzing customer and transaction data, and identifying suspicious transactions based on automated triggers and constantly updated customer/partner profiles.
- KYC utilities based on DLT or other technology are also included in this area of RegTech.

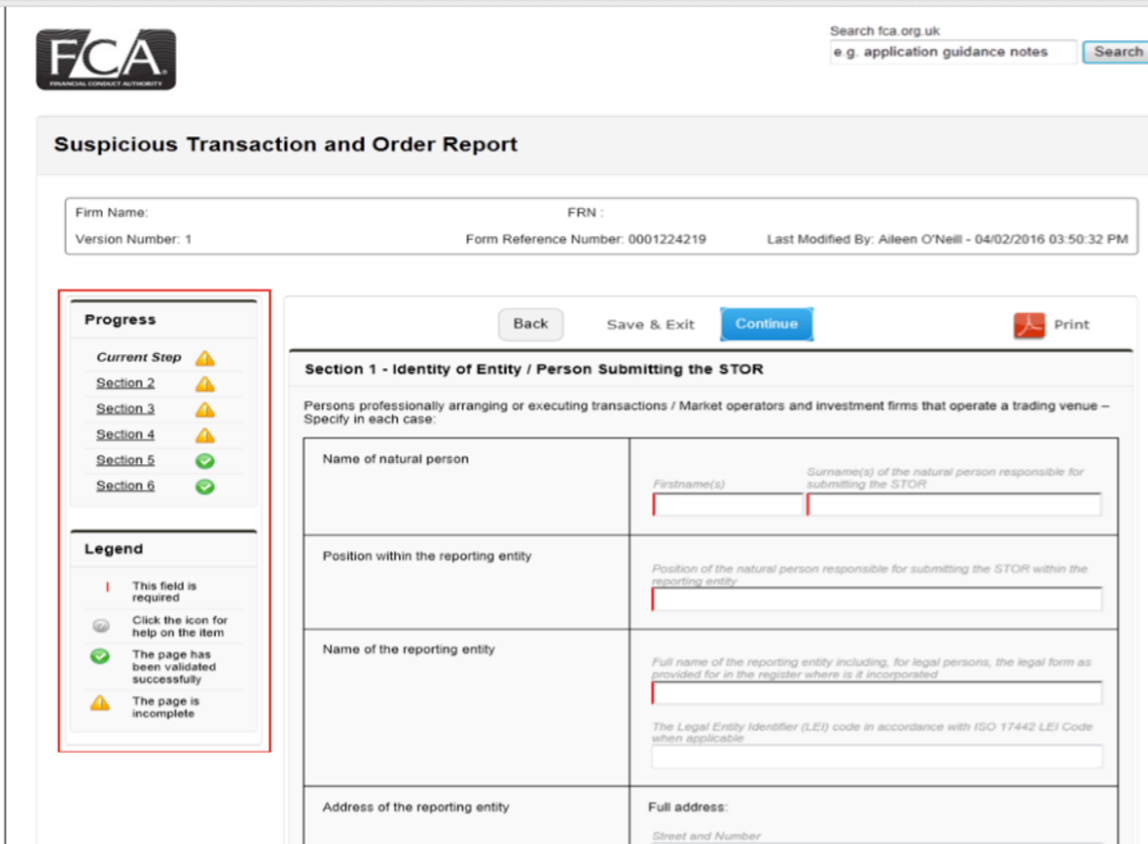
Example: Spending monitoring

- The input consists of data from a bank or payment cards.
 - The responses, (or output), are the handheld purchases made. They include an open banking interface that draws in data from a bank account.
 - Input data is used to train a classification model to identify the spending.
 - Since the goal is classification, it applies supervised learning.
- Log data for day 1 and store it in a text file labelled “Spending.”
 - On day 2 store the same data in a second text file labelled “Spending2.”
 - Repeat the steps for a month to identify each spending activity.
 - Store the labelled data sets in a text file. A flat file format such as text or CSV is easy to work with and makes it straightforward to import data.
 - Divide the data into two sets. Save one set of the data for testing (the test set) and use the rest (the training set) to build models. This is referred to as holdout, and is a useful cross-validation technique.

Suspicious transaction reports

- Banks spend 40B USD on AML annually while catching less than 1% of the proceeds from money-laundering, which amounts to over 2.5 trillion USD every year.
- Legacy AML systems are inefficient, outdated, and lead to heavily manual processes.
- The use of cryptocurrency and the digitization of money brings new challenges for compliance officers.

ns-information/suspicious-transaction-order-report-stor-connect-guide.pdf



FCA Search fca.org.uk
e.g. application guidance notes Search

Suspicious Transaction and Order Report

Firm Name: FRN :
Version Number: 1 Form Reference Number: 0001224219 Last Modified By: Aileen O'Neill - 04/02/2016 03:50:32 PM

Back Save & Exit Continue Print

Section 1 - Identity of Entity / Person Submitting the STOR

Persons professionally arranging or executing transactions / Market operators and investment firms that operate a trading venue – Specify in each case:

Name of natural person	Firstname(s) Surname(s) of the natural person responsible for submitting the STOR
Position within the reporting entity	Position of the natural person responsible for submitting the STOR within the reporting entity
Name of the reporting entity	Full name of the reporting entity including, for legal persons, the legal form as provided for in the register where it is incorporated The Legal Entity Identifier (LEI) code in accordance with ISO 17442 LEI Code when applicable
Address of the reporting entity	Full address: Street and Number

Progress

Current Step ⚠

Section 2 ⚠

Section 3 ⚠

Section 4 ⚠

Section 5 ✓

Section 6 ✓

Legend

- ⚠ This field is required
- 🔍 Click the icon for help on the item
- ✓ The page has been validated successfully
- ⚠ The page is incomplete

Source: FCA

Pseudo-anonymity

- Bitcoin and other cryptocurrencies have a public transaction history.
- Techniques such as context discovery and flow analysis can be used to investigate suspicious activity.
- In Oct 2019, 337 suspected criminals were arrested across 38 countries following tracing of their cryptocurrency accounts.

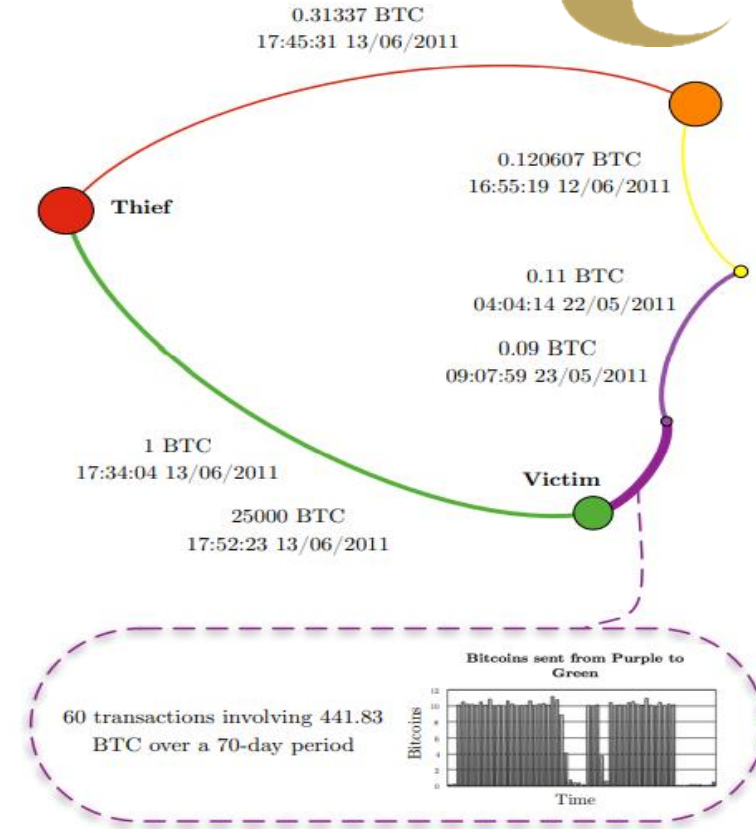


Fig. 1.12: An interesting sub-network induced by the thief, the victim and three other vertices. The notation is the same as in Fig. 1.11.

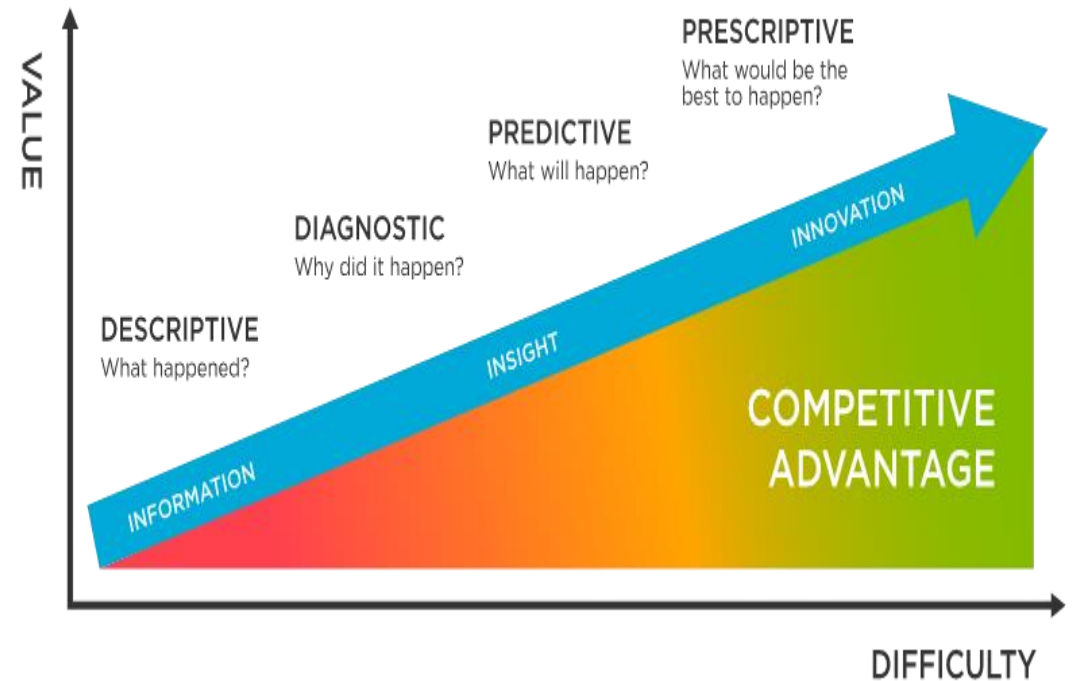
Data sharing



- Data sharing is often accomplished through an application programming interface (API).
- Data sharing in financial services tends to be risk and permissionbased, with required audit trails, and subject to regulation and risk management.
- Payment Initiation Service Providers (PISPs) and Account Information Service Providers (AISPs) have interfaces with financial institutions.
- Right to privacy: GDPR (General Data Protection Regulation) imposes a substantial penalty for noncompliance

Conclusion

- The digital revolution is an exogenous shock. There has been dramatic innovation in digital communications, robotics, information processing and analytics.
- Communication technology, information storage and data processing are key to regulatory success.
- Moving from descriptive, through diagnostic, to predictive and prescriptive compliance.



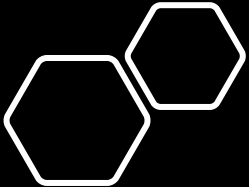
Source: TIBCO Software Inc.

The Role of Technology & PPPs in Fighting Financial Crime

Inspector Steven Meighan BL, Garda
National Economic Crime Bureau (GNECB)
FIU Ireland

CPD CODE: 2022-0012





(Informal) Public Private Partnership

Joint Intelligence Group Ireland





Successes

Cardless Cash Lodgments

- STR analysis, Discussed at JIG and solution proposed

Quality of STRs

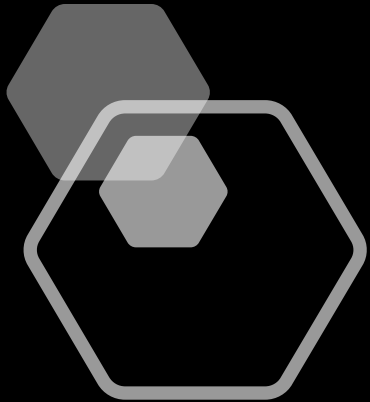
- Feedback at JIG, better quality STRs with keywords that can be prioritised

Specific Operations

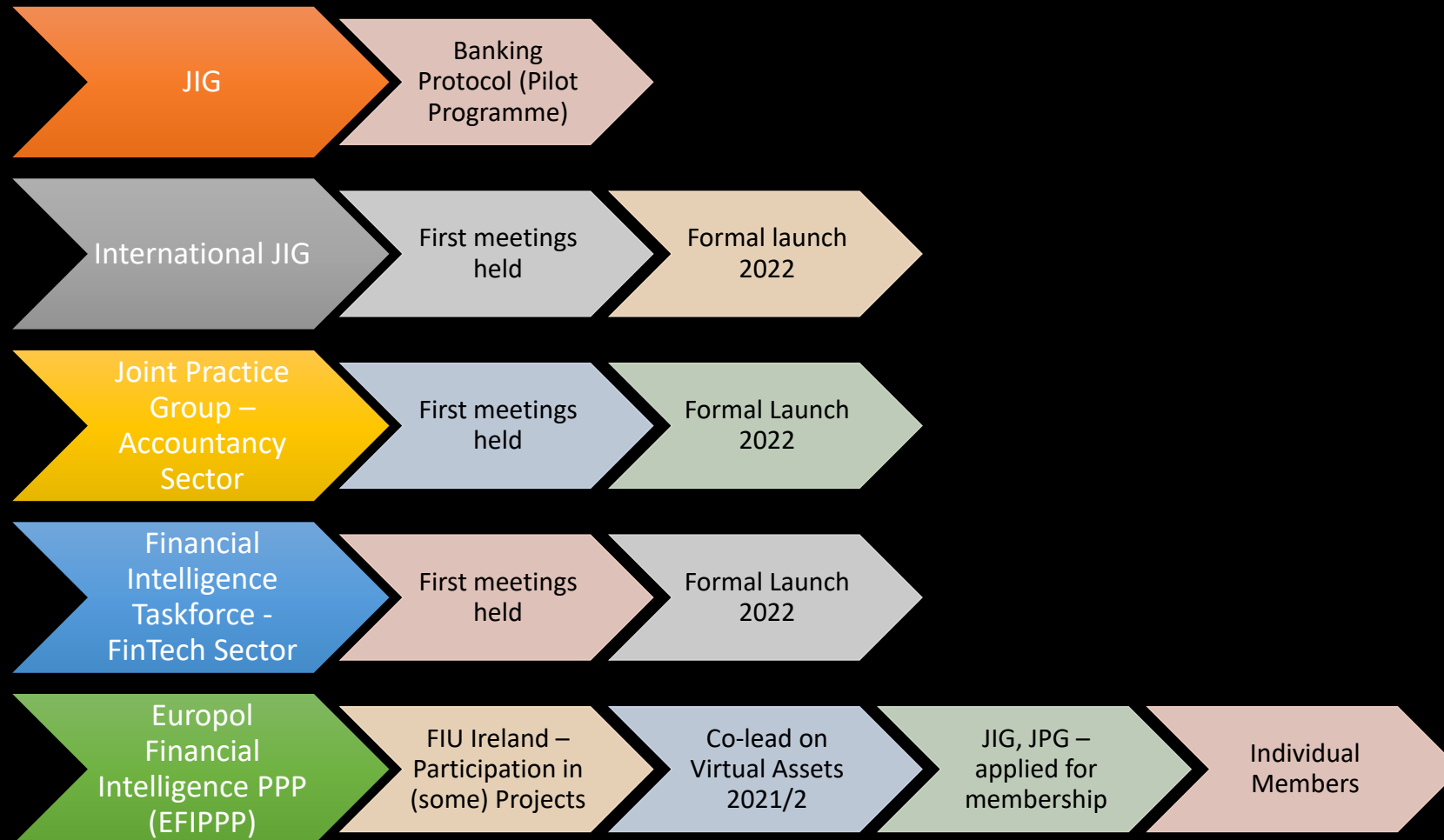
- JIG informed what we are looking for, STRs sent in with Operation name

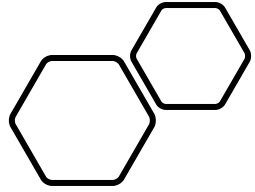
Specific Examples

- Ireland/Holland
- Ireland/Sweden
- Ireland/Luxembourg



Follow on PPPs in Ireland





Contact Details

steven.j.meighan@garda.ie

garda.ie

fiu-Ireland.ie

www.linkedin.com/in/stevenmeighan

Micro-Creds

What are Mirco-Creds?



Professional Certificates (10 ECTS @ Level 8 on the NFQ)

Delivered on-line over 12 weeks (3 hours per week)

Accredited in partnership with Technological University Dublin

Delivered by professionals for professionals

Practical contemporary industry focused learning environment

Option to 'stack' ECTS in a major (Diploma) award

Why Micro Creds?



Key Features

Opens up more agile & flexible learning opportunities

Focuses upon the targeted acquisition of specific skills and competences

Key Benefits

Enables professionals to build upon on their knowledge/experience without having to completing a full higher education programme

Enables professionals to upskill or reskill to meet evolving labour market demands and develop professionally

Find Out More?



Starting week of Monday February 7th 2022

<https://fintech.pat.edu.eu/product/professional-certificate-in-fintech-aml-compliance-framework>

<https://fintech.pat.edu.eu/product/professional-certificate-in-fintech-aml-cycle/>

<https://fintech.pat.edu.eu/product/professional-certificate-in-fintech-evolution-of-aml-compliance/>

<https://fintech.pat.edu.eu/product/professional-certificate-in-fintech-innovation-regtech/>

Thank You For Attending The Role of Technology & Public Private Partnerships in Fighting Financial Crime

A recording of this webinar and
the CPD code will be available on
our website later today.

CPD CODE: 2022-0012



Questions?