PRIVACY ENHANCING TECHNOLOGIES & THEIR POTENTIAL FOR GLOBAL IMPACT

Rob Leslie, Founder and CEO, Sedicii

Webinar

Friday, 30 July 2021, 11:00 BST

A Word From Today's Chairman

Robert Pay

Senior Associate

Z/Yen Group

FS Club

Platinum Sponsors

Invest Northern Ireland
CDI China Development Institute
Finance Montréal
AIFC
Seoul Together we stand
Busan Finance Center
HK Financial Services Development Council 香港金融發展局
LuxembourgforFinance Agency for the Development of the Financial Centre
ADGM An International Financial Centre
Dubai International Financial Centre
The Government of Moscow
The Department for External Economic and International Relations of Moscow

Gold Sponsors

Aptitude Software
BRIDGEWORKS
FEATURE SPACE
OUTSMART RISK
ARBORETUM
Crown Agents Bank
CERIDIAN
ENTRUST

Silver Sponsors

Bottomline
GPS global processing services
BCS CONSULTING Expect Excellence
P2 CONSULTING
The Technium Global SERVICE WITH INTEGRITY
expert.ai
CLOUDSOFT
PRAXITY Empowering Business Globally

Bronze Sponsors

Profile Software
(expleo)
CONTACT PARTNERS
alyne
ESTATES AND INFRASTRUCTURE EXCHANGE

Personal Sponsors

Challenge Curve
Currencycloud
worldpay
mastercard
RADIX
ZB
LEI Global Legal Entity Identifier Foundation
cuff associates PART OF THEBES GROUP
Volanté
TRANSPARENCY TASK FORCE
CYGNETISE
Catalina Consulting
AMSOM
GIBRALTAR STOCK EXCHANGE

Today's Agenda

- 11:00 – 11:05 Chairman's Introduction
- 11:05 – 11:25 Keynote Presentation – Rob Leslie
- 11:25 – 11:45 Question & Answer

Today's Speaker

Rob Leslie

Founder and CEO

Sedicii

sedicii

Privacy Enhancing Technologies & Their Potential For Global Impact

www.sedicii.com

@gbrsedicii

sedicii

6th June, 2013

sedicii

Cambridge Analytica

sedicii

Cambridge Analytica

GDPR

What are Privacy Enhancing Technologies?

PETs are a variety of cryptographic techniques and protocols, architectural designs, data workflows, and systems of hardware and software that enable organisations to **collaborate on sensitive data without needing to rely on mutual trust**.

Source: Lunar Ventures

What are Privacy Enhancing Technologies?

Homomorphic Encryption – cryptographically ensures that both the data and the result of a computation remain secret, removing the need to trust the location where the computation happens.

Secure Multi-party Computation – enables multiple, mutually-untrusting parties to collaborate on a joint computation on confidential data, preventing any participant from learning anything about the inputs provided by the other parties.

Differential Privacy – Its main goal is to protect the privacy of an individual who is providing his information to a database that is used for aggregate analysis.

Source: Lunar Ventures

What are Privacy Enhancing Technologies?

Zero Knowledge Proofs – allows data provided by one party to remain secret while being verified by another party. Can be used as an auditing system which allows the underlying information not to be exposed.

Synthetic Data – is an artificial data set that mimics the properties and relational characteristics of a genuine, confidential data set.

Federated Machine Learning – delivers machine learning models to the locations where the data is stored to perform the training locally removing the need to store all data in a centralised location.

Trusted Execution Environments (TEE) – is a hardware partition that secures the execution environment completely from the rest of the processing unit.

Source: Lunar Ventures

sedicii

What problems do PETs solve?

Handling sensitive data and sharing it with third parties imposes large liabilities which have prevented us from exploiting the full potential of the data ecosystem.

PETs enable data collaborations using confidential data without needing to trust the parties involved in that collaboration.

e.g. Healthcare, Financial Services, Law Enforcement, Cybersecurity

Source: Lunar Ventures

What Opportunities do PETs create?

PETs adoption could unlock **a trillion dollar opportunity** by helping us extract more value from existing data, by enabling a new generation of services and use-cases to flourish.

Source: Lunar Ventures

sedicii

What Opportunities do PETs create?

McKinsey estimates that only 1% of the world's data is being used for analysis.

Two things to note:

1. At least **10% of the $11.5T value** of the digital economy is based on analysing that 1% of data.

2. PETs will allow us to utilise an additional 1% (at least) of the data available over the next 20 years and extract at least another 10% of value - **that's $1-2 Trillion** of new value!

Source: Lunar Ventures, McKinsey 2015

What Benefits can PETs offer?

PETs' main goal is to increase the level of confidentiality when multiple parties collaborate together on sensitive data.

PETs drastically improve the trade off between generating value from data and respecting its secrecy but, depending on the technology chosen, can incur efficiency losses in doing this.

Source: Lunar Ventures

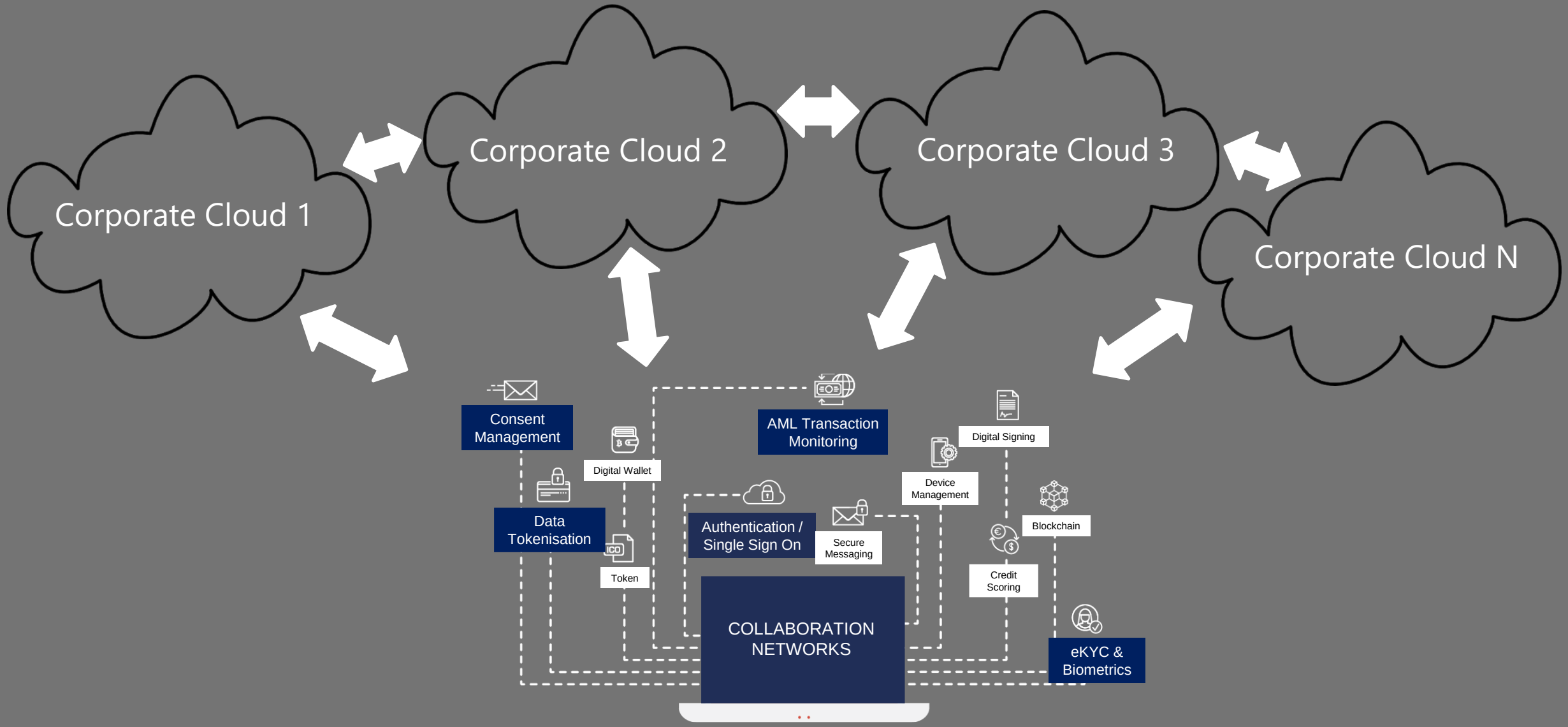
sedicii

Where can the inefficiencies arise?

- **Computational overhead** – Computation on encrypted data is heavy
- **Communication overhead** – Lots of parties mean lots of messages
- **Network Latency** – Processing can take time to conclude
- **Integration & Engineering complexity** – Tasks may require expert resources to design and build
- **Legal & Governance** – Collaborations require legal frameworks to operate which can take time to put together

Source: Lunar Ventures

Collaboration Networks – Clouds' next great transformation



IDENTITY IS THE FOUNDATION OF EVERYTHING

Audience Poll

Would your business benefit from the use of Privacy Enhancing Technologies?

a) Very significantly
b) Significantly
c) Somewhat
d) Not so much
e) Not at all

Privacy Enhancing Technology Landscape

	Encryption	Information-Theoretic Secure
Trusted Execution Environments (TEE)	✓	✗
Homomorphic Encryption (HE)	✓	✗
Multi-Party Computation (MPC) (different flavours)	✓	✓
Zero-Knowledge Proofs (ZKP)	✗	✓

Can Leak Information

Random Noise

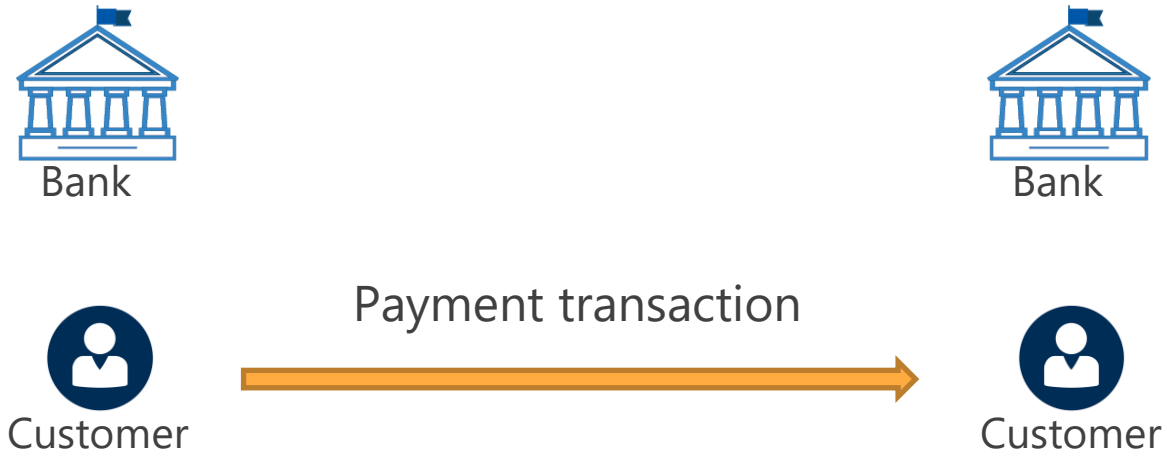
$$\text{random string} = \alpha \oplus \textit{data string}$$

Perfect Secrecy:

The random string does not leak any information about the string of data, *even if the attacker is equipped with infinite computational resources and time.*

- Encryption and hashing may leak information
- One-time-padding will not leak any information

Example: Transaction Monitoring in the Context of AML



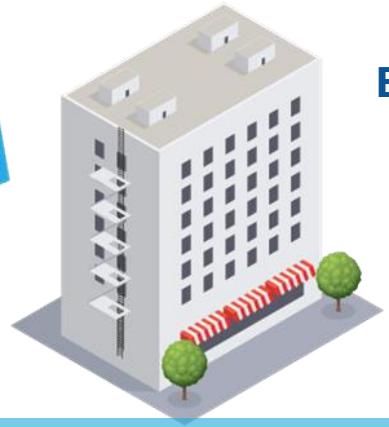
What is the Fraud / Money Laundering Risk associated with the transaction?

Example: Transaction Monitoring in the Context of AML

If banks could communicate with each other, to **create insight** legally, on a transaction or an account, **without sharing any customer data**.....

Account Detail
Transaction Detail
Activity Detail

Bank A



Bank B

....they could intelligently and confidentially identify behaviours, traits and characteristics at the Sender and Receiver Banks to generate **RISK SCORES & ALERTS**

Example: Transaction Monitoring in the Context of AML

Transaction Activity

- Number of outgoing payments
- 1st party payment range
- Frequency of payments
- Rapid movement of funds
- Number of cash deposits
- Number of cross border payments

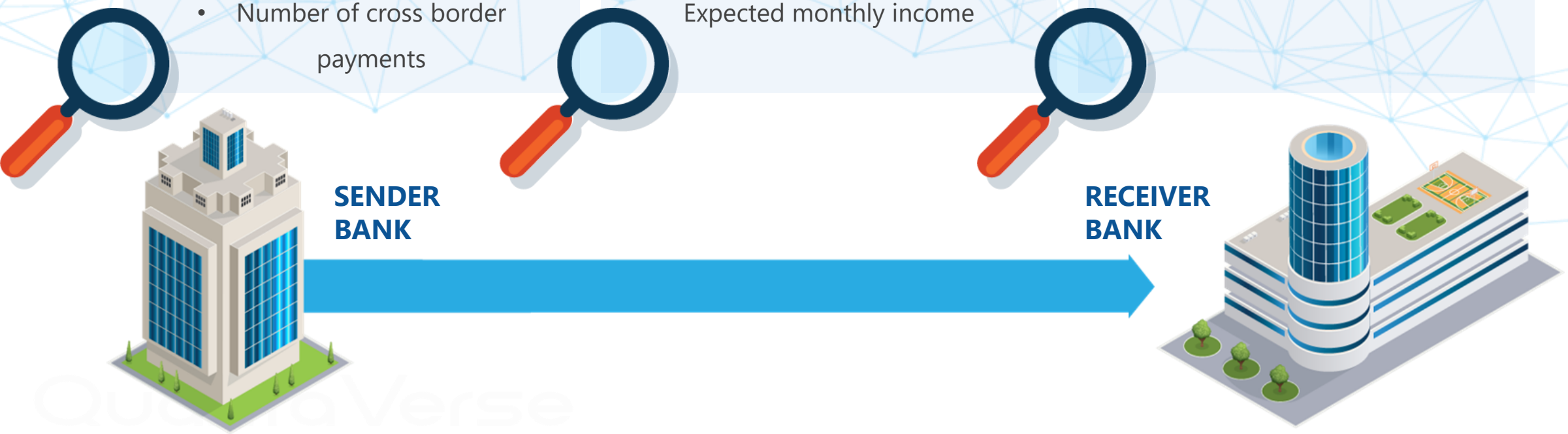
Client Attribute Profile

- Age range (if applicable)
- Gender (if applicable)
- Net worth
- Employment status
- Wealth profile (£,€,$)

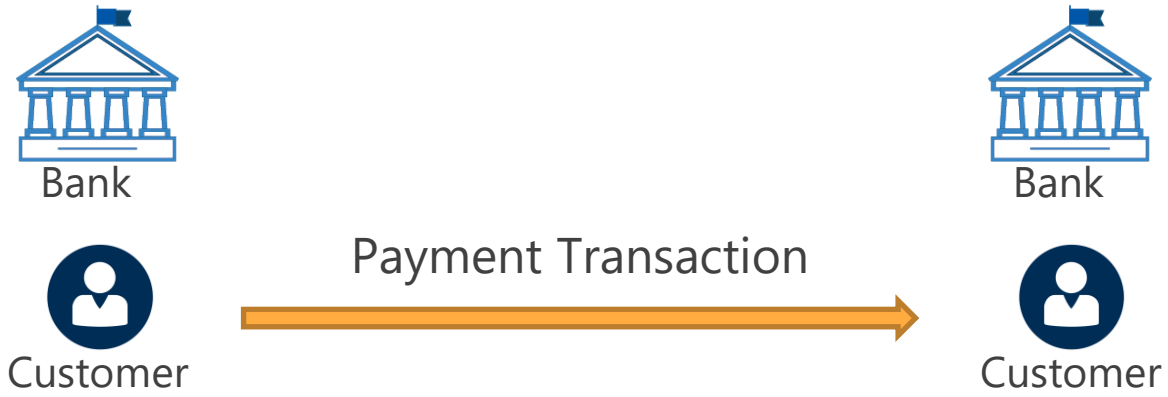
Expected monthly income

Login Activity / History

- Typical bank log in medium
- Typical IP address
- Typical region of activity
- Time of banking activity

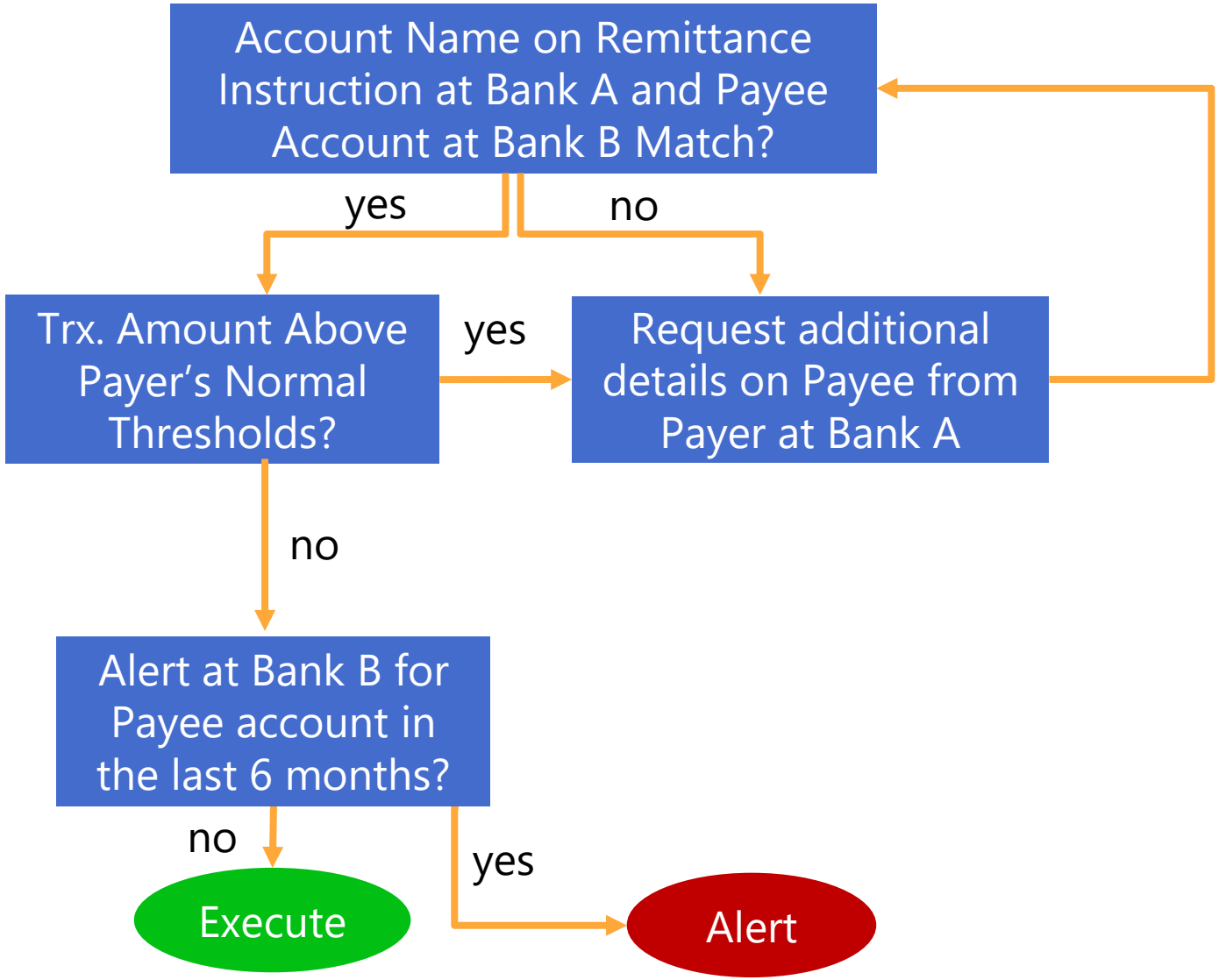


Example: Transaction Monitoring in the Context of Fraud / AML



What is the AML / fraud risk associated with the transaction?

Real World Problem – Authorised Push Payment Fraud



sedicii | Prexa | Identity and Suitability demo | Which role do you play? (•) Bank A ( ) Bank B | USE CASE: APP Fraud | FCA FINANCIAL CONDUCT AUTHORITY

Bank A Payment Instruction Data - Ashleigh Scott

Name	British Telecom
Account Number	40250872
BIC	AIBKIE2D
Address	1, Canada Sq. Canary Wharf
Postcode	E14 5AB
Country	United Kingdom

Bank B - Identity check

Name	Russell Hunter
Account Number	40250872
BIC	AIBKIE2D
Address	Walton, Liverpool
Postcode	L4 5RL
Country	United Kingdom

Bank A - Suitability checks

Is the account holder resident in the UK	NO	YES
Has the account been active for more than one year	NO	YES
Has a SAR been filed in the last year	NO	YES
Is volume of transactions in last month higher than normal	NO	YES
Has a hold been placed on this account in the last year	NO	YES

Bank B - Suitability checks

Is the account holder resident in the UK	NO	YES
Has the account been active for more than one year	NO	YES
Has a SAR been filed in the last year	NO	YES
Is volume of transactions in last month higher than normal	NO	YES
Has a hold been placed on this account in the last year	NO	YES

sedicii | Prexa | Identity and Suitability demo | Which role do you play? (•) Bank A ( ) Bank B | USE CASE: APP Fraud | FCA FINANCIAL CONDUCT AUTHORITY

Bank A Payment Instruction Data - Ashleigh Scott

Name	British Telecom
Account Number	40250872
BIC	AIBKIE2D
Address	1, Canada Sq. Canary Wharf
Postcode	E14 5AB
Country	United Kingdom

Bank B - Identity check

Name	Russell Hunter
Account Number	40250872
BIC	AIBKIE2D
Address	Walton, Liverpool
Postcode	L4 5RL
Country	United Kingdom

The collaborative algorithm identifies account data at the beneficiary Bank B that does not match the remittance instruction at Bank A.

Note the different account name and address in Bank B for the same account number in Bank A

Once the difference is identified the transaction is automatically stopped

Bank A - Suitability checks

Is the account holder resident in the UK	NO / YES
Has the account been active for more than one year	NO / YES
Has a SAR been filed in the last year	NO / YES
Is volume of transactions in last month higher than normal	NO / YES
Has a hold been placed on this account in the last year	NO / YES

Bank B - Suitability checks

Is the account holder resident in the UK	NO / YES
Has the account been active for more than one year	NO / YES
Has a SAR been filed in the last year	NO / YES
Is volume of transactions in last month higher than normal	NO / YES
Has a hold been placed on this account in the last year	NO / YES

Audience Poll

What do you see as the greatest barrier to the deployment of Privacy Enhancing Technologies in your organisation?

a) Legal and Regulatory uncertainty around data
b) Lack of technical knowledge and understanding
c) Unwillingness to collaborate with others
d) Cost is too high
e) Benefit to the organisation is insufficient

Possible Use Cases

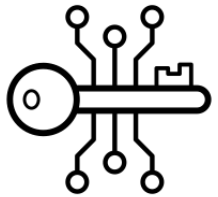
AML and fraud risks can be confidentially calculated using data contributed by all parties involved in a transaction

Insurance Claim Fraud and other risks can be calculated to see if a similar claim has been submitted to another insurance company by the same individual

Confidential Data Analytics can be generated using inputs from multiple parties where the inputs are not disclosed to other parties in the group

Health insurance claims made by an individual can be confidentially verified at healthcare providers and pharmacies

Credit Reports can be automatically calculated at the point of sale using data confidentially contributed by different service providers



Protection of Cryptographic Keys used in the signing of digital documentation and instructions

sedicii

Rob Leslie

CEO

rob.leslie@sedicii.com

www.sedicii.com

@gbrsedicii

Comments, Questions & Answers

FS Club

Platinum Sponsors

Invest Northern Ireland
CDI China Development Institute
Finance Montréal
AIFC
Seoul Together we stand
Busan Finance Center
HK Financial Services Development Council 香港金融發展局
LuxembourgforFinance Agency for the Development of the Financial Centre
ADGM An International Financial Centre
Dubai International Financial Centre
The Government of Moscow
The Department for External Economic and International Relations of Moscow

Gold Sponsors

Aptitude Software
BRIDGEWORKS
FEATURE SPACE
OUTSMART RISK
ARBORETUM
Crown Agents Bank
CERIDIAN
ENTRUST

Silver Sponsors

Bottomline
GPS global processing services
BCS CONSULTING Expect Excellence
P2 CONSULTING
The Technium Global SERVICE WITH INTEGRITY
expert.ai
CLOUDSOFT
PRAXITY Empowering Business Globally

Bronze Sponsors

Profile Software
(expleo)
CONTACT PARTNERS
alyne
ESTATES AND INFRASTRUCTURE EXCHANGE

Personal Sponsors

Challenge Curve
Currencycloud
worldpay
mastercard
RADIX
ZB
LEI Global Legal Entity Identifier Foundation
cuff associates PART OF THEBES GROUP
Volanté
TRANSPARENCY TASK FORCE
CYGNETISE
Catalina Consulting
AMSOM
GIBRALTAR STOCK EXCHANGE

Thank You For Listening

Forthcoming Events

- Mon, 2 Aug (15:00-15:45) CCPs: You'll Never Walk Alone?
- Tue, 3 Aug (10:00-10:45) Augmenting The Augmentors - How The Great Western Metaverse Will Be Built
- Thu, 5 Aug (11:00-11:45) A World Of Individual Opportunity: The Vision Of Egalitarian Capitalism

Visit https://fsclub.zyen.com/events/forthcoming-events/