secretarium

Leveraging Secretarium For Real-Time Fraud and Scam Detection in Interbank Payments

Version: 1.2 – May 2024

Author: Bertrand Foing

Abstract

In the modern landscape of financial transactions, Authorised Push Payment (APP) fraud has emerged as a significant threat to both financial institutions and their customers. With the rise of digital banking and online transactions, fraudsters have exploited vulnerabilities in traditional payment systems, resulting in substantial financial losses and reputational damage. In response to this challenge, multiple financial institutions are exploring innovative solutions to combat APP fraud while preserving data privacy and confidentiality. This white paper examines the problem of APP fraud and proposes a collaborative platform for real-time fraud detection and prevention.

www.secretarium.com

Contents

Introduction

In recent years, the financial industry has witnessed a surge in Authorised Push Payment (APP) fraud, posing significant challenges to financial institutions and their customers. APP fraud occurs when individuals are deceived into authorising the transfer of funds from their own accounts to those of fraudsters.

> ***"APP scam losses are expected to hit $6.8 billion by 2027".***
> **ACI Worldwide Scamscope**

Despite efforts to prevent and detect APP fraud, it remains a pervasive threat, leading to substantial financial losses and eroding trust in financial institutions. Fraud detection methods, such as rule-based systems and transaction monitoring, have limitations in identifying sophisticated fraudulent activities in real-time. As a result, financial institutions are increasingly turning to innovative data collaboration approaches to enhance their capabilities. However, legal barriers, such as those related to data privacy, and difficulties around the ownership and governance of cross-jurisdiction facilities, have prevented the emergence of global solutions.

By allowing data to be processed in encrypted form, Secretarium enables secure computation without exposing sensitive information to unauthorised parties or compromising competitive integrity. In this white paper, we propose a promising platform for fraud detection in interbank payments, leveraging the collaborative computing capabilities of Secretarium to compute risk ranks in real-time, and enabling financial institutions to proactively identify and mitigate fraudulent transactions.

1 Understanding APP Fraud

1.1 Definition and Types of APP Fraud

Authorised Push Payment (APP) fraud refers to fraudulent schemes in which individuals are deceived into authorising the transfer of funds from their own accounts to those of fraudsters. Unlike unauthorised transactions, where funds are taken without the account holder's consent, APP fraud involves the victim willingly transferring money under false pretences. This type of fraud encompasses various tactics and schemes, including:

- **Impersonation Scams**: Fraudsters impersonate trusted entities such as banks, government agencies, or service providers to deceive victims into making payments. Common methods include phone calls, emails, or sms claiming urgent issues or rewards requiring immediate payment.
- **Invoice Fraud**: Fraudsters send fake invoices or payment requests to individuals or businesses, tricking them into transferring money for goods or services that were never provided.
- **Romance Scams**: Fraudsters establish fake romantic relationships with victims online, gaining their trust and eventually convincing them to send money for fabricated reasons such as medical emergencies or travel expenses.
- **Investment Scams**: Fraudsters lure victims with promises of high returns on investments, persuading them to transfer money into fraudulent schemes or fake investment opportunities.
- **CEO Fraud/Business Email Compromise**: Fraudsters impersonate company executives or suppliers, tricking employees into authorising payments or transferring funds to fraudulent accounts.

1.2 Impact on Financial Institutions and Customers

The impact of APP fraud extends beyond financial losses, often causing emotional distress, reputational damage, and loss of trust in financial institutions. Victims may suffer not only financial hardship but also psychological harm from the betrayal of trust and the realisation of being deceived.

For financial institutions, APP fraud results in direct financial losses due to reimbursing victims, as well as indirect costs associated with investigating fraud cases, implementing fraud prevention measures, and managing reputational damage.

1.3 Challenges in Detecting and Preventing APP Fraud

Detecting and preventing APP fraud presents significant challenges for financial institutions due to the evolving nature of fraudulent schemes. Fraudsters techniques to evade detection are continuously getting more sophisticated, making it challenging to keep pace. Some social engineering tactics, such as impersonation scams and phishing attacks, can deceive even vigilant customers and frontline staff.

Fraudsters are not elusive masterminds. Financial institutions could thwart even the most sophisticated fraud attempts if they weren't constrained by fragmented efforts. Challenges such as banking secrecy, stringent data protection regulations, and privacy laws require institutions to balance fraud prevention with maintaining rightful customer privacy, greatly limiting their capabilities.

Moreover, fraud often involves cross-border transactions and international networks of fraudsters, complicating efforts to trace and prosecute perpetrators. Jurisdictional challenges and differences in legal frameworks across countries hinder the ability to investigate and prosecute fraud effectively, creating opportunities for fraudsters to operate with impunity.

1.4 Data Collaboration Example

Here is a simple example of how signals and insights could be shared between financial institutions to stop scammers luring payments into Barbara's taken over / mule account.

Alistair is lured into paying Barbara and is the victim of a scam. His Bank A shares a suspicious scam activity report.

Bank B receives the report, investigates Barbara's recent behaviour, and discovers an unusual flow of funds. Bank B shares a suspicious mule account report.

Chloe is also lured into paying Barbara. Bank C uses the available insights to convince Chloe to cancel the payment and shares a suspicious scam activity report.

David is in another jurisdiction and is also a victim of this international scam. Bank D data collaboration service is interconnected with other jurisdictions', allowing the same insights to convince David to cancel the payment.

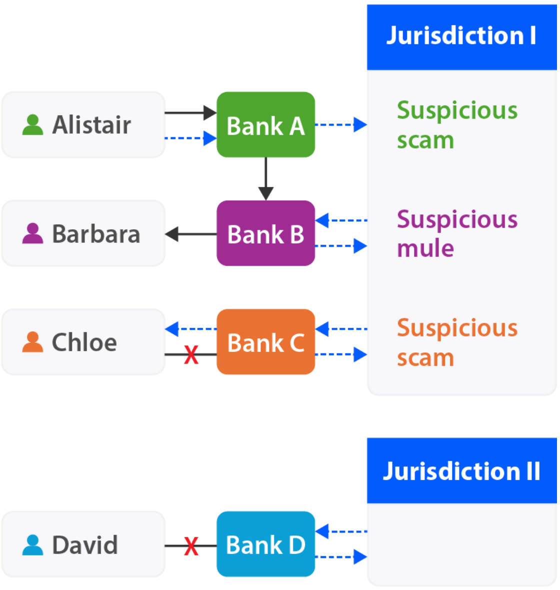


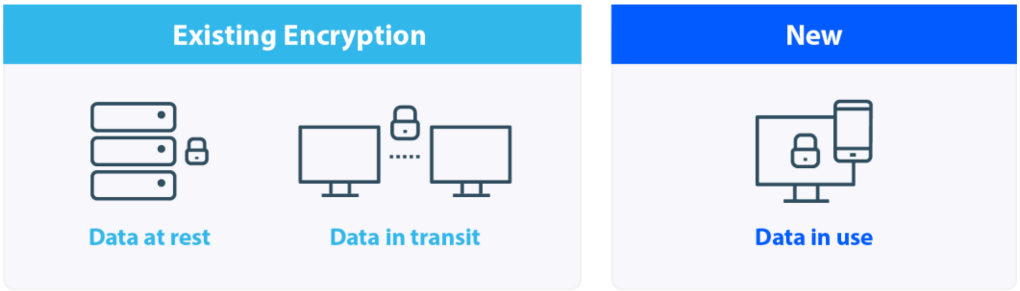
Fig 1: Cross-jurisdiction data collaboration.

2 Overview of Secretarium Technology

Secretarium is a leading provider of confidential computing solutions, offering advanced technology to safeguard sensitive data and ensure privacy and security in digital environments.

2.1 Confidential Computing

Confidential computing is a paradigm in computing that focuses on protecting data while it is being processed. Traditional computing models typically involve data being encrypted when at rest or in transit, but decrypted when in use, leaving it vulnerable to potential breaches during processing.



Confidential computing addresses this vulnerability, thus minimising the risk of exposure to unauthorised parties. It also protects the processing in a demonstrable way, a fundamental feature that Secretarium uses as a building foundation for honest-by-design services.

Key principles		
Encrypted Memory Data remains encrypted while in memory, preventing unauthorised access by other processes or users.	**Secure Enclaves** Hardware-based security mechanisms, such as Intel SGX, create isolated environments within the CPU known as "enclaves," where sensitive computations can be performed securely.	**Tamper-proof Execution** Any attempts to tamper with a secure enclave's memory or code are detected and prevented, ensuring that the computation remains secure and tamper-proof.
Benefits		
Confidentiality Confidential computing enables sensitive computations to be performed without exposing raw data to the underlying infrastructure or third-party service providers, reducing the risk of data breaches and safeguarding the confidentiality of proprietary information.	**Integrity** Secure enclaves ensure the integrity of data and code, allowing businesses to have confidence in the accuracy and reliability of the outcomes produced. This reliability allows businesses to make informed choices based on trustworthy data analysis and insights.	**Collaboration** Financial institutions can collaborate securely on sensitive data without sharing plaintext information, enabling joint analysis and decision-making while preserving data privacy.

2.2 Demonstrating Data Protection

Secretarium harnesses the power of a comprehensive suite of privacy-enhancing technologies (PETs) to empower financial institutions in safeguarding their most sensitive information. Through a strategic combination of multi-party computing (MPC), confidential computing, and differential privacy, Secretarium enables organisations to establish robust safeguards for their data assets, and compliance with data protection by design and by default guidelines.

Secretarium also offers a clear platform to deliver attestable and tamper-proof services. This secure transparency is achieved with a unique combination of confidential computing and distributed ledger technology, on top of which it provides a zero-trust applicative runtime to continuously verify the identity of every component, application, user and device. By anchoring every applicative transaction deterministically onto a distributed ledger, Secretarium ensures integrity and immutability of both data and process, thus enhancing trust, accountability and auditability in a code-is-law fashion. This provides the demonstrable guarantees of neutrality, a fundamental enabler of shared ownership.

These features make Secretarium the most effective cloud-native tool for solving complex problems ranging from data privacy to regulatory compliance, collaborative computing, digital asset and credential custody, tokenisation, and many more.

2.3 Real-time Messaging

Secretarium's engineers, many of whom have extensive experience in low-latency trading systems, recognise the critical role of real-time solutions. In 2018, we introduced the pioneering privacy-preserving data collaboration solution, DANIE, to financial institutions. DANIE enables instant responses to queries and supports real-time subscriptions and push notifications.

Fraud and scams demand swift action. Payment service providers (PSPs) must assess the risk of unknown payees within milliseconds to uphold user experience standards. Secretarium meets this demand by leveraging distributed ledger technology, allowing it to scale and support thousands of queries per second. In terms of latency, confidential computing has almost seamless performance overheads, it is orders of magnitude faster than any other PETs.

Real-time monitoring of behavioural data, such as amounts, payees, login patterns and frequencies, allows for the detection of suspicious deviations, such as those associated with account takeover or mule accounts. Reporting these changes in risk ranks in real-time enables other financial institutions to promptly alert users and prevent fraud.

By leveraging real-time messaging capabilities, Secretarium empowers financial institutions to respond swiftly to evolving threats, enhancing fraud detection and prevention efforts while maintaining user trust and security.

2.4 Unified Ledger

A Unified Ledger is a concept proposed by the Bank for International Settlements (BIS) to revolutionise the global financial system. It refers to a network of interconnected systems designed to seamlessly integrate various components of the financial ecosystem, addressing the persistent challenges of fragmentation, inefficiency, and lack of interoperability.

While the original vision of the Unified Ledger focuses on facilitating value exchange across borders, currencies, and asset classes, the Secretarium technology emerges as a pivotal enabler in this paradigm shift for advanced risk management and fraud detection.

Secretarium capabilities in data protection, tamper-proofing, and transparency offer a particularly well-designed solution to support jurisdiction-based systems, tailored to adhere to local regulations. These systems can be customised to accommodate jurisdiction-specific data requirements and typologies.

Through its scalable architecture, its advanced customisation around data collaboration, and by interconnecting these jurisdiction-specific systems, Secretarium proposes the creation of a Unified Ledger dedicated to facilitating a concerted effort to combat fraud and scams on a global scale.

3 Data Collaboration Platform

Jurisdiction-tailored facilities for data collaboration can be interconnected to form a unified ledger.

3.1 Overcoming Siloed Approaches

An effective solution for combating fraud and scams goes beyond individual risk management systems operated by payment service providers (PSPs) in isolation. While various privacy-enhancing technologies (PETs) have been explored over the years, some approaches have proven to be unsuitable due to their limitations in facilitating collaborative data analysis and correlation.

Keeping data siloed may seem simpler from a regulatory and compliance standpoint, but it inherently limits the effectiveness of fraud detection efforts. Pooling data from multiple sources allows for the aggregation of diverse information, the temporality, and the correlation of data points, enabling the early detection of patterns and anomalies. Only by analysing comprehensive insights from PSPs can potential fraud indicators be created, and suspicious activities accurately detected.

In contrast, maintaining data silos prevents the capture of these correlations. Query-based and federated approaches, even when protected by PETs such as homomorphic encryption, multi-party computing, differential privacy, or federated learning are inappropriate in scenarios where data pooling is essential for the effective transformation of weak signals into risk ranks.

By moving beyond siloed approaches and embracing collaborative data pooling, Secretarium allows organisations to leverage the collective intelligence of multiple stakeholders and enhance fraud detection capabilities.

3.2 Secure Data Ingestion

Collecting the right data is crucial for effective detection and prevention of fraud and scam, but this needs to be done in a privacy-preserving fashion.

Data collaboration necessitates the use of unique identifiers to facilitate the aggregation and correlation of data from diverse sources. Bank accounts are typically identified by numbers, country codes, sort codes, routing numbers, and branch codes, with some adhering to standards like the ISO 13616 for International Bank Account Numbers (IBANs).

By constructing a unique identifier for each account, organisations can attach metadata such as internal risk scores, alerts, changes in behaviour, owner presence on public records such as watchlists, politically exposed persons (PEP) lists, or sanctions lists. Secretarium's privacy-enabling technology ensures that this information is securely pooled while demonstrating data protection by design and by default.

Secretarium's technology also provides the framework for integrating data validation mechanisms seamlessly into the data ingestion pipeline, verifying the accuracy and completeness of data before it is processed or used for decision-making, and enhancing the reliability and trustworthiness of the data used for fraud detection and prevention.

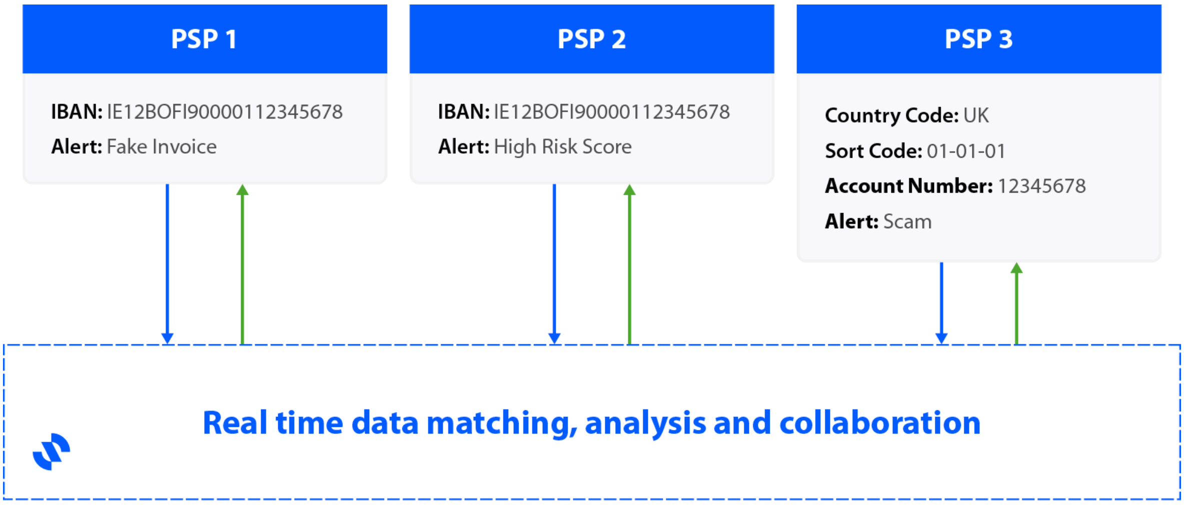


Fig 2: Data collaboration with different identifiers.

While the primary responsibility for risk management lies with each PSP's system, there are no technical barriers preventing the expansion of data ingestion beyond banking data. For instance, integrating additional identifiers like phone numbers could enable the utilisation of Telco APIs, enhancing risk assessment in real time based on factors such as the account owner's interaction with a suspicious caller. Centralising such integrations could distribute costs among participating parties, making them more feasible and beneficial for all involved.

3.3 Programmability and Purpose Limitation

Secure enclaves offer unparalleled flexibility as they are fully programmable, allowing institutions to tailor data collaboration strategies to their specific needs. Unlike other PETs that impose rigid constraints on business logic, Secretarium empowers institutions to design and implement sophisticated algorithms at silicon speed.

This flexibility allows parties in each jurisdiction to implement the collaborative rules, the analytics engines, the AI models, the cheat lists, and all possible intelligence-generating business logic they want and need to detect and prevent financial crime in real time.

Secretarium’s combination of programmability and encryption is paramount in ensuring that data is collected and processed only for specific, legitimate purposes. It allows the enforcement of typology restrictions, as well as granular access control policies based on data ownership or user roles.

Furthermore, secure enclaves are auditable by design, with attestations providing verifiable assurance of their security and integrity. These attestations can be shared with auditors or regulators to demonstrate compliance with data protection requirements and provide transparency into the security measures implemented to protect sensitive data.

3.4 Data Accuracy

Trust is paramount in any data collaboration service, necessitating robust measures to ensure the accuracy and integrity of the data and processes involved. Secretarium employs advanced techniques to safeguard data integrity, preventing unauthorised modifications throughout the processing lifecycle.

Utilising clusters of interconnected secure enclaves, Secretarium is a transactional system managing distributed, encrypted, and tamper-proof ledgers. This architecture guarantees that data remains accurate and consistent, providing assurances of integrity at every stage of processing.

Furthermore, it enables the enforcement of audit trails, offering a transparent record of all interactions and operations within the collaborative solution. By tracking data modifications, Secretarium provides a comprehensive record of the state of the collaborative environment, bolstering trust and confidence in the accuracy and reliability of the data collaboration service.

3.5 Compliance with Tipping-Off Regulations

Identifying potentially suspicious accounts early empowers financial institutions to proactively prevent fraudulent activities and mitigate financial and reputational risks. By flagging accounts displaying unusual behaviour patterns or indicators of fraud, participants signal their peers to take additional security measures.

Tipping-off regulations prohibit financial institutions from disclosing suspicions of money laundering or terrorist financing to customers or third parties, as this could compromise ongoing investigations or tip off perpetrators. To navigate this challenge, Secretarium proposes unique strategies:

- **Encrypted Ledgers**: Maintaining the underlying data of collaborative solutions fully encrypted, and using tamper-proof secure enclaves to enforce the data access governance, prevents unauthorised access to both external and internal users.
- **Context Enforcement**: To mitigate internal illegitimate accesses, queries can be restricted to payment workflows only, preventing internal users to query arbitrary bank accounts.
- **Recipients Tracking**: Tracking users' interactions with suspicion alerts can facilitate investigations into tipping-off incidents and aid in perpetrator detection.

3.6 Compliance with Data Protection Regulations

A bank account identifier is a personally identifiable information (PII). To comply with the General Data Protection Regulation (GDPR), and equivalent regulations worldwide, consent for third-party data processing is necessary. This typically isn't a major obstacle, given that most customers consent to third-party data processing for fraud management when opening a bank account.

However, as a failsafe measure and since GDPR principles don't govern anonymous data, Secretarium provides an advanced technique for anonymising PII on-premise. This method relies on a local secure enclave provisioned with an anonymisation secret owned by the remote collaboration system. This ensures the continued matching of encrypted anonymised data from some PSPs with the encrypted original data from others.

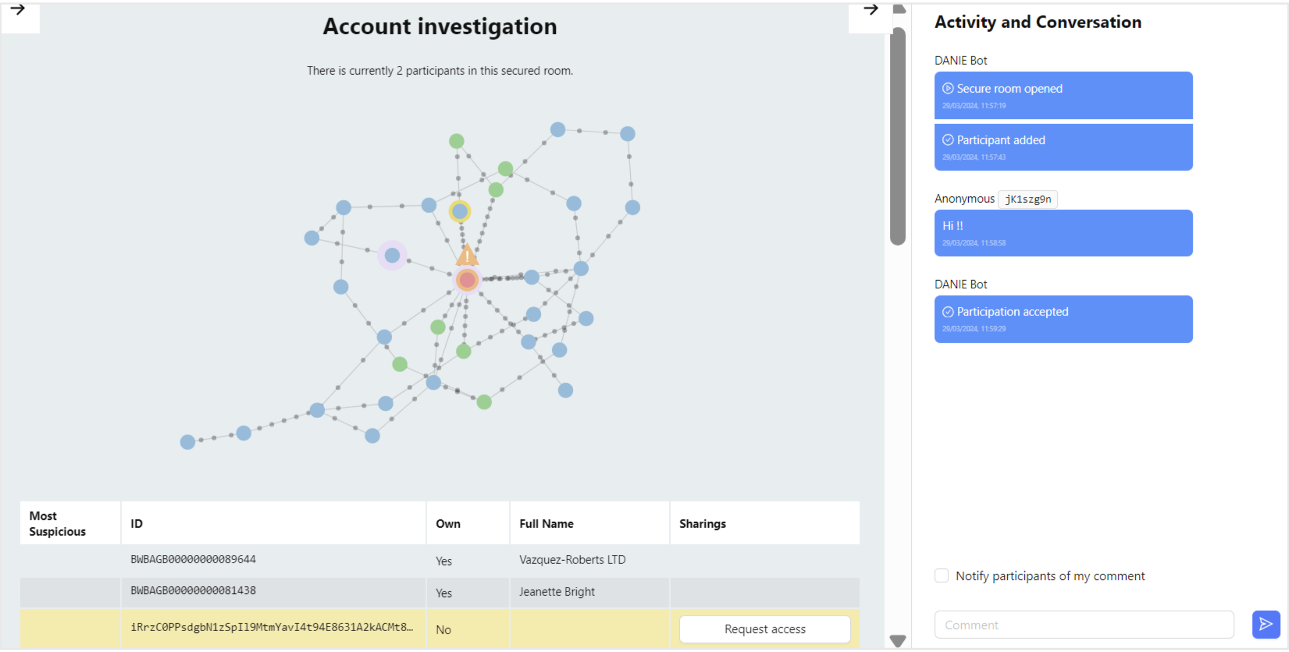
It is also important to note that GDPR does not explicitly address the classification of encrypted information. To date, no EU/EEA court has issued a definitive ruling on whether encrypted data should be considered personal or not. Nonetheless, the highest authority for data protection regulation in

Bavaria, the Landesamt für Datenschutzaufsicht, has determined that encrypted data does not meet the criteria for personal data if encrypted using robust state-of-the-art cryptographic methods.

By implementing rigorous security and privacy measures, by offering the flexibility to deploy advanced strategies and adopt risk-based approaches, Secretarium empowers PSPs to leverage data collaboration effectively while demonstrating adherence to industry best practices and efforts to comply with relevant regulations and standards.

3.7 Secure Rooms for Investigations

The Secretarium platform facilitates interactive exploration and analysis of findings through confidential secure rooms, accessible to participating PSPs. These secure environments allow PSPs to launch a collaborative investigation on an account and invite peers that have also raised a suspicion.



Account investigation

There is currently 2 participants in this secured room.

Most Suspicious	ID	Own	Full Name	Sharings
	BWBAGB00000000089644	Yes	Vazquez-Roberts LTD	
	BWBAGB00000000081438	Yes	Jeanette Bright	
	iRrzC0PPsdgbN1zSpI19MtmYavI4t94E8631A2kACMt8…	No		Request access

Activity and Conversation

DANIE Bot

Secure room opened
29/03/2024, 11:57:19

Participant added
29/03/2024, 11:57:43

Anonymous jK1szg9n

Hi !!
29/03/2024, 11:58:58

DANIE Bot

Participation accepted
29/03/2024, 11:59:29

□ Notify participants of my comment

Fig 3: Secure rooms example (here for AML investigations based on graph network topologies).

These joint examinations significantly enhance each institution's internal intelligence capabilities. In the secure room, more extensive data sharing can occur securely. They feature an encrypted live chat functionality to facilitate discussions.

Secure rooms are fully anonymous, all parties are assigned ephemeral identifiers that are unique for each new secure room instance. They offer the ability to invite local authorities or agencies to join the investigation and further increase the collective effort.

3.8 Integration with Existing Systems

The proposed solution is designed to seamlessly integrate with the existing fraud management systems of participating financial institutions. Leveraging APIs and easy-to-integrate protocols, the solution facilitates interoperability, empowering institutions to enhance their existing infrastructure with augmented fraud detection capabilities.

The solution fosters collaboration between jurisdiction-specific systems deployed by different financial institutions. By bridging these jurisdiction-specific systems, the solution fosters a networked approach to fraud data collaboration. Through secure communication channels, the Unified Ledger routes queries, alerts and relevant insights while adhering to regulatory requirements and data privacy standards.

Conclusion

In the ever-evolving landscape of financial crime and fraud, the need for robust and innovative solutions has never been more pressing. The challenges faced by financial institutions in combating authorised push payment (APP) fraud and scams demand innovative approaches that can adapt and evolve in real time to protect financial institutions and their customers.

The persistence of financial crime highlights the limitations of traditional fraud detection methods and underscores the critical need for a proactive, collaborative, and technologically advanced solution. The proposed approach, rooted in the principles of confidential computing and privacy-enhancing technologies (PETs), offers a transformative pathway to real-time fraud detection and prevention in interbank payments.

By enabling customer privacy, by safeguarding data integrity, and by facilitating secure data collaboration, Secretarium empowers financial institutions with the building foundations for new financial crime services. These collaborative approaches enable institutions to leverage collective insights, signals, and intelligence, augmenting their ability to identify and respond to emerging threats.

Furthermore, the integration with existing systems and the adoption of a unified ledger approach enables seamless interoperability between jurisdiction-tailored systems, fostering cross-system and cross-border collaboration. This global scale platform is complemented with secure rooms to enable advanced investigations, facilitate controlled data disclosure between institutions and in-depth analysis of suspicious activities.

As financial crime continues to evolve, embracing innovative solutions like the proposed approach is essential for staying ahead of threats and protecting the interests of institutions and customers alike. The time has come for financial institutions to collectively innovate and collaborate, leveraging cutting-edge technology to address fraud and scams holistically. Together, let us forge a future where financial crime is systematically detected, all while preserving the rightful privacy of financial institutions' customers.

Contact

Bertrand Foing, Secretarium

Email: bertrand@secretarium.org

References

G20 भारत 2023 INDIA

Secretarium won the BIS / G20 Techsprint 2023 competition on fighting money laundering, combating financing of terrorism, tax and sanctions evasion.

ACPR BANQUE DE FRANCE

Secretarium and FutureFlow competed at the ACPR/Banque de France Techsprint 2022 and won the competition against the most advanced PETs companies.

A-Team Innovation Awards from A-Team Group

Most innovative data privacy by design award 2023.
Most innovative financial data security solution 2021.
Most innovative use of distributed ledger technology 2021.

Danie

Secretarium powers the suite of DANIE solutions since 2018. These solutions have been used by 15 of the largest financial institutions and millions of records have been processed.

www.secretarium.com