PREVENTING FINANCIAL FRAUD ACROSS DIFFERENT JURISDICTIONS WITH SECURE DATA COLLABORATIONS

IMDA PET SANDBOX – MASTERCARD CASE STUDY

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

Contents

Business Case

1. **Mastercard, a global technology company in the payments industry**, via its Cyber and Intelligence Solutions business line has been assessing the potential for frontier technologies, including Privacy Enhancing Technologies (PETs), to buttress its product offerings against financial crimes like money laundering.

2. **Mastercard developed a proof of concept (POC) in IMDA's PET Sandbox program** to investigate a product based on Fully Homomorphic Encryption (FHE), provided by a third-party supplier, for sharing financial crime intelligence across international borders – specifically between Singapore, the United States ("US"), India and the United Kingdom ("UK") – while complying with prevailing regulations.

Methodology

3. **The POC** simulated the use case scenario where two or more Mastercard entities would exchange data among themselves or with third parties (e.g., banks) in the context of cross-border financial crime monitoring and prevention.

4. An "inquiring entity" would "query" a "source entity" as to whether a specific "inquiry data" i.e. the International Bank Account Number ("IBAN") has been flagged by the "source entity" as high risk. The "results" from source entity will be a Boolean output, i.e. "True/False"

5. **Test data was used**, generated completely at random using a so-called "faker" library in the Python programming language. No real data was used to generate the test data, nor used to validate. The databases on each source entity node were re-generated using the same algorithm for each test.

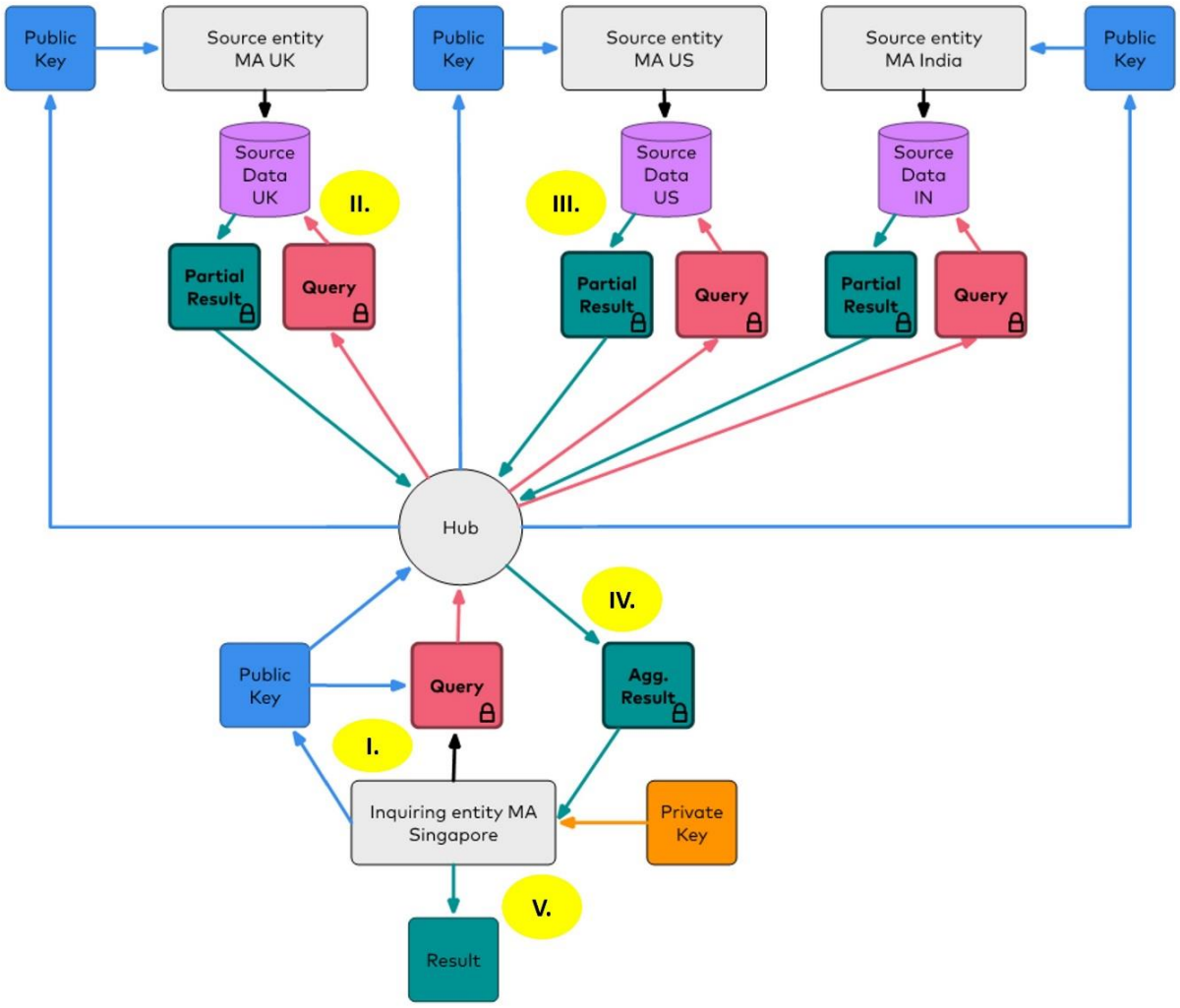
Solution Architecture

6. **FHE was used for this POC** given its ability to share insights between parties without one party learning about the questions being asked by the other, and without the underlying data being accessed by the inquiring party. This was especially useful for anti-money laundering use case and the fight against international organised crime groups, as the technology enables financial intelligence between and within organisations while

ensuring compliance with regulatory requirements relating to the disclosure and transfer of that information.

7. **The POC solution architecture** was designed to enable the following sequence of events (also see Figure 1):
   I. The inquiry data is encrypted using a public key held by the inquiring entity and used to query the source entities via hub.
   II. The hub distributes the secure query to all source entities, where FHE-based operation is performed on the source data.
   III. The source entities respond with an encrypted result (the source data does not leave its environment), which are sent back to the hub for aggregation.
   IV. The hub sends the aggregated-encrypted result back to the inquiring entity.
   V. The inquiry entity decrypts the aggregated-encrypted result using its private key.

Figure 1 – Solution Architecture



Legal and Regulatory Considerations

8. The POC solution was assessed against **key legal requirements in 4 countries** – specifically, the U.S., the UK, India, and Singapore. The legal analysis below, based in part on the advice given to Mastercard by external legal advisers, considered the possibility for an entity to both be an inquiring entity as well as a source entity.

9. **Cross-border data transfer or data localization requirements** which may prevent the inquiring or source entities from engaging in cross-border transfer of or overseas storage of personal data or financial data. An IBAN and information relating to it was assessed against considerations that could amount to personal data under the data protection laws of Singapore, India, the US, and the UK even when encrypted[1], potentially triggering cross-border data transfer or data localisation requirements.

    i. **Singapore:** Mastercard is certified under both the Asia Pacific Economic Cooperation Cross Border Privacy Rules System ("CBPR"), and Privacy Recognition for Processors System ("PRP") for intra-group transfers. Mastercard would also be able to rely on contractual safeguards with non-certified companies. The Personal Data Protection Act 2012 ("PDPA") does not contain data localization requirements. In the context of Singapore, the solution offers the benefit of facilitating compliance with security requirements related to transfers (e.g., the obligation to protect personal data in transit).

    ii. **India[2]:** Under the IT Rules 2011, the inquiry data, and the source data (but not the results) will likely be considered as Sensitive Personal Data or Information ("SPDI"). The transfer of SPDI is permitted if the data is transferred to a country that provides the same level of protection as the IT Rules 2011, and if the transfer is consented to by the data subject, or is necessary for the performance of a contract. This means that the POC solution would enable disclosures of SPDI to third parties (even cross-border). There are no general data localization requirements under Indian law, however there are data localization requirements specific to the payments sector, laid down in the Reserve Bank of India's ("RBI") Storage of Payment System Data directive. This requires Mastercard (as well as any bank licensed in India) to store data relating to payment systems in servers or systems only in India. The RBI's FAQs

[1] Laws considered: Singapore's Personal Data Protection Act 2012 ("PDPA") was considered, India's Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 as well as the Reserve Bank of India ("RBI") Storage of Payment System Data directive, US's Gramm-Leach-Bliley Act ("GLBA") as well as any other state privacy law currently in force, and UK's General Data Protection Regulation ("UK GDPR").

[2] The activities in the sandbox were conducted prior to the issuance of the Digital Personal Data Protection Act 2023, and hence do not consider the implications arising from it, but it is worthwhile noting that the DPDP Act adopts a negative list approach to countries to which data can be sent to.

to the directive further clarify that there is no bar on processing of payment transactions outside India, but the data must be deleted from the systems abroad no later than one business day or 24 hours from payment processing (whichever is earlier), and the data must be stored only in India after the processing. The FAQs further mention that "any subsequent activity such as settlement processing after payment processing, if done outside India, shall also be undertaken / performed on a near real time basis". Where a source entity is located in India, it only receives the encrypted query and generates the results. Therefore, in the context of the POC, the results do not appear to fall under the scope of the RBI directive. More regulatory clarity will however be required where an inquiring entity is located in India. While the query containing the IBAN is encrypted and indecipherable to the source entity, and the query does not persist outside of India for longer than 2 minutes as the query is being processed, further clarification will be required to determine whether the directive and FAQs would allow for the sending of the encrypted query using FHE.

iii. **U.S.:** There were no cross-border data transfer or data localization requirements as of the development of this POC. As a result, implementing the solution would not impact Mastercard's compliance with any U.S. cross-border data transfer or data localization requirements.

iv. **UK:** Mastercard Europe Services Limited has binding corporate rules ("**BCRs**") in place which have been authorised by the Information Commissioner's Office ("**ICO**"), to lawfully perform transfers from the UK for fraud, or authentication and financial crime purposes. For transfers from the UK, where BCRs cannot be used, Mastercard will need to enter into an additional agreement[3]. Irrespective of the transfer mechanism used, Mastercard will need to carry a transfer risk assessment. In the UK, the ICO has recognised the use of the technology of the solution to provide "enhanced protection" in circumstances where a risk is identified[4].

10. **Data protection requirements**, including the legal basis to process personal data, and the sharing of information with third parties for the inquiring entity or the source entity; and individuals' rights under the data protection laws to access and correct data collected by the inquiring entity.

i. **Singapore:** In Singapore, implementing the FHE solution may assist Mastercard in relying on the "legitimate interests" basis to process inquiry data, source data and the result, given the purpose to prevent illegal activities such as financial crime.

[3] Mastercard will either need to enter into a UK International Data Transfer Agreement or add the UK Addendum to the EU's Standard Contractual Clauses.

[4] Accessible at https://ico.org.uk/media/for-organisations/documents/4022649/transfer-risk-assessments-tool-20221117.doc

ii. **India:** Implementing the solution will not affect the legal bases available to Mastercard under Indian law. Mastercard will need to rely on a legal basis under the law (e.g., consent, or under contract) to collect or disclose the data.

iii. **U.S.:** Implementing the solution does not materially influence Mastercard's choice of legal basis when processing personal data for financial crime monitoring and prevention purposes. U.S. privacy laws generally permit processing for the purposes of fraud prevention, even if the information is not encrypted.

iv. **UK:** Legitimate interest will be the most likely applicable legal basis and the solution would help Mastercard demonstrate it has implemented safeguards to minimise the risk to the individuals.

11. **Confidentiality requirements** which may be imposed on the inquiring or source entities (e.g., a bank) which are subject to legal and compliance requirements relating to the sharing of data offshore and/or to third parties such as Mastercard.

i. **Singapore:** The Banking Act prohibits disclosure of 'Customer Information' (CI). If the outputs (True/False) to the query run on encrypted IBANs inadvertently divulges the existence of a (non-public) relationship between the customer and the bank, that would likely constitute disclosure of CI. Conversely, if the FHE solution enables a bank to disclose information that is not referable to any named customer or group of named customers, for example, by aggregation such that the inquiring entity cannot identify a relationship between a bank and a customer, the bank would not be in breach of secrecy of CI.

ii. **India:** The solution reduces the volume of potentially confidential information being shared in the context of conducting financial crime monitoring and prevention activities. Indian banking secrecy rules would apply if Mastercard were to onboard any banks licensed in India as source or inquiring entities. Even so, the solution could enhance Mastercard's ability to comply with secrecy obligations as minimal customer information is shared (e.g., True/False predefined results) using the solution, and the shared customer information is encrypted. As for the sharing of inquiry data, should banking secrecy requirements apply, exceptions could be relied upon e.g., financial crime monitoring and prevention could be in the interest of the bank.

iii. **US:** The solution does not materially influence Mastercard's compliance with confidentiality restrictions. The GLBA permits the sharing of non-public personal

information with both affiliated and non-affiliated entities for the purposes of protecting against fraud.

iv. **U.K.:** the solution would not avoid a duty of confidentiality, and disclosures would need the individual's authorisation. Even so, the solution reduces the amount of confidential information disclosed and implements a safeguard using FHE to preserve the confidentiality of the information disclosed.

12. **Anti-money laundering (AML) requirements** that might apply to the use case and whether the Mastercard solution circumvents any impediments or restrictions presented by such laws. However, for all jurisdictions in scope, no challenges on AML and KYC reporting requirements were identified in the POC. Further analysis would be required depending on the participating entities to the solution.

Technical and Governance Assessment

13. The POC was tested against data field lengths, computation time, complexity of queries and governance arrangements which a solution may need to support.

14. **No Significant Effect of Data Field Lengths**: The size of the IBAN had no significant effect on the round-trip time as long as there was memory capacity on the data nodes. An identifier twice as large as a normal IBAN (44 characters) was tested, which was sufficient to simulate the expected range of the encrypted predicate string length.

15. **Node Locations affect Computation Time**: Nodes in Ohio (US), Mumbai (India) and London (UK) were tested in the POC to study the impact of geography on round-trip time (the amount of time it takes for a query submitted to the Hub to return a response back to the Hub). It is worth noting that each node scaled in the same manner as the number of rows to query at that node. For comparable queries, the fastest round-trip time was about 100 seconds for querying 1 million records, limited by the node located furthest (Ohio) from the Hub (Singapore).

16. **Method of processing queries with FHE-encrypted predicates differs from traditional query processing.** Queries with a mix of FHE-encrypted and non-encrypted predicates, or "compound queries", must be written such that non-encrypted predicates are processed before executing the remainder of the query using an encrypted predicate. This helps speed up the time required to complete the query and return the encrypted result. Table 1 below explains how this differs from the way "traditional queries" are processed. The range of queries tested in the POC are described in Table 2.

Table 1 – Processing Traditional Queries vs Compound Queries

	Traditional Queries (without encrypted predicates)	Compound Queries (including FHE encrypted predicates)
Sequence	Exclude as much of the index as possible first, followed by filters on the other fields.	Process the non-encrypted predicate first, then filter that subset down to just the IBAN of interest.
Example	Implement the high-risk query first to filter out any rows that do not share an IBAN with the query, then filter down to rows that have a risk greater than the threshold.	Find all the IBANs with risk greater than the threshold, then filter out any rows that do not share the IBAN with the query.

Table 2 – Queries executed in the POC

Query ID	Query	Encrypted Predicate	Non-Encrypted Predicate	Result
Q1	Does IBAN exist in any country?	IBAN	None	Boolean
Q2	Does IBAN exist in any country with a score greater than a risk threshold?	IBAN	Risk threshold	Boolean
Q3	Is the aggregated transaction value for this IBAN greater than a value threshold?	IBAN	Value threshold	Boolean
Q4	Is the Account Open date for this IBAN within a particular number of days?	IBAN	Day range	Boolean

17. **Necessary Governance Arrangements to keep the system honest:** Basic enterprise governance and security arrangements were considered for an FHE-based product.

i. Encryption Key Governance

- Three types of keys are used for all FHE-related computations to assure the security and privacy of the data and model in use: Public Key (to encrypt data, query, or model), Private Key (to decrypt query results), and Evaluation Public Keys (to perform calculations based on homomorphic operations).

- Access to specific types of keys depends on the role of participating entity. For the POC, all three keys were generated by the inquiring party, each set generated per query. It is also possible for the Evaluation Public Key to be cached at the source entity for a configurable amount of time to reduce the cost of each query.
- In relation to financial data, a best practice is to use Hardware Security Modules (HSMs) to manage cryptographic keys. However, homomorphic keys are not typically supported by standard HSMs at the point of this POC and are ephemeral. As such, a key manager compatible with FHE would need to be considered for the future.

ii. **Source Data Governance** – Governance of the content of the participating source entities, in this case IBAN under watchlist, would need to be put in place in order to safeguard the integrity of the results of queries e.g. keep the watchlist up to date, standardise data formats towards incoming queries, have compliance teams safeguard the watchlist against unauthorised access or use.

Conclusions and Next Steps

18. The POC let Mastercard conclude that FHE holds promise. A useful and effective user experience can be facilitated by an API built on top of today's FHE powered technology. However, deploying it in an enterprise environment is not without challenge. Existing governance processes may need to be updated to accommodate how FHE keys are managed and how the source data is maintained. Choice of node locations may be limited by business considerations of participating source entities, affecting the speed of completing queries and taking action to quell illicit activities.

19. Generally, the use of FHE in the 4 legal jurisdictions considered in this POC has a positive impact in the areas of cross-border data transfers, data localisation, and data protection laws. There are specific regulatory requirements in the context of banking secrecy and data localization which will need to be further clarified. Some of these concerns may be addressed by enveloping the product with governance controls (e.g. pre-approved list of queries, aggregation of query outputs before decryption).

20. Taking lessons from the POC, Mastercard will continue to explore a set of use cases, both domestic and international, that use FHE to provide value to customers with heightened security postures around sensitive queries.