ISSUE BRIEF

U.S. POLICY

PETs Use Case:

Preventing Financial Fraud Across Different Jurisdictions with Fully Homomorphic Encryption

Organization: Mastercard

FUTURE OF PRIVACY FORUM

Problem:
Like other international financial services organizations that manage cross-border transactions, Mastercard must often prioritize responding to and disrupting fraud. In this specific case, Mastercard is interested in determining if a particular account number – International Bank Account Number (IBAN) – has a sufficiently high fraud score to constitute "high risk." The traditional method of checking to see if fraud was present would involve multiple round-trips of cross-border data sharing (Send IBAN > Store IBAN > Check IBAN against local records > Compute if the risk score is above the limit > return IBAN + results to the originator). This process requires careful balancing of legal requirements in three different areas: data transfer/data localization, data protection, and confidentiality.

Current Fraud Detection Method

Mastercard designed a system to limit the amount of information both querying and receiving parties may view, ideally resulting in a simple true/false response returned to the querying entity. More directly, a query originating in one country can get responses about the risk of a given IBAN from multiple other countries without sharing the IBAN itself. Further, the sharing countries do not need to share their underlying risk scores - they can instead simply notify the querying entity whether or not a given IBAN is above or below the line.

Proposed PET Details

Technology Type:

- The core PET in this use case is **fully homomorphic encryption (FHE)** of the IBANs being queried and risk score analysis results.
- In addition to FHE, this use case utilizes a **query "hub" system** that can provide aggregates of responses. Thus, a querying entity could know simply that an IBAN was flagged *somewhere,* but not from where.
- This solution would require systems to enable encryption key governance and mechanisms to ensure the source data in each remote location is correct and appropriately limited.
- This solution would benefit from Hardware Security Modules (HSMs) to support the management of FHE keys; however, they do not currently exist.

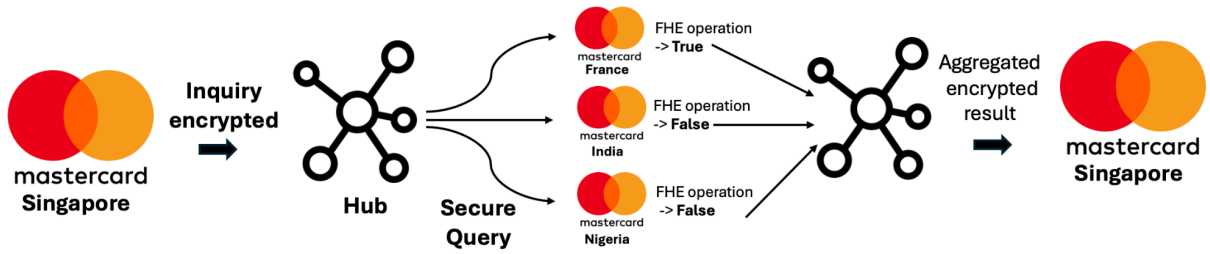
Functionality:

- In this case, the work proceeded in five steps:
    a. The inquiry data is encrypted using a public key held by the inquiring entity, which is used to query the source entities via the hub.

b. The hub distributes the secure query to all source entities, where FHE-based operations are used to query the source data without exposing the queried IBANs to the source entities or exposing any data apart from the approved response to the inquiring entity.
c. The source entities respond with an encrypted result (the source data does not leave its environment), which is sent back to the hub for aggregation.
d. The hub sends the aggregated encrypted result back to the inquiring entity.
e. The inquiry entity decrypts the aggregated-encrypted result using its private key.

- This use case is designed to protect data subjects' privacy and reduce unintended harms to them, in part via a strictly limited purpose. By highlighting a single and specific purpose (fraud detection), the system described can enable fraud checks without sharing any additional information. As it is not multi-purpose, any additional utility would need to be subsequently designed.

Fraud Detection Method Using Fully Homomorphic Encryption (FHM)



Beneficiaries of enabling lawful cross-border, privacy-preserving fraud checks:

- Consumer: Ultimately, consumers pay for fraud through higher prices charged by service providers when their costs (e.g., insurance) increase. Further, consumers benefit from the system's privacy protections, as access to their personal data is limited, and the system prevents an inquiry from becoming a cause for further investigation because a log cannot be created of their IBAN being checked.
- Financial institutions: Financial institutions benefit from reducing fraudulent transactions through lower costs, such as reducing liability, insurance premiums, legal compliance, and customer dissatisfaction.
- Governments: Multiple agencies within national governments are typically tasked with reducing fraudulent transactions that impact their citizens, be these direct theft from individuals or money laundering-type transactions. Systems enabling fraud checks while remaining in compliance with other laws reduce the likelihood of fraud, ultimately decreasing the time and resources spent on fraud prevention or reduction. Additionally, there is a wider benefit of building trust in payments and the digital economy.

Industry/Domain(s):
Financial services; Law enforcement

Stakeholders:
Mastercard and the Singapore Infocomm Media Development Authority ("IMDA") were involved in the test described in this use case.

Background and Motivation:
In this case, Mastercard proposes using Fully Homomorphic Encryption ("FHE") to enable the transmission of IBANs to remote destinations to check against local risk scores. It also proposes that the remote destinations return an encrypted boolean TRUE or FALSE (TRUE meaning the IBAN was a "high risk" IBAN or FALSE, not a "high risk" IBAN) so as not to reveal to the sharing entity what information was queried. FHE is a PET that allows for computation on encrypted data without requiring the data or the query to be decrypted.[1] Using FHE, Mastercard hopes to enable fraud checks across multiple jurisdictions without sharing any IBANs or information that may be unlawful to transfer, share, or otherwise transmit.

Current Regulatory Environment:
Mastercard assessed the proposed PET solution against key legal requirements in four countries: 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 be both an inquiring entity and a source entity. This section is taken directly from the published IMDA PET Sandbox report.[2]

Cross-border data transfer or data localization requirements 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 were assessed to determine if they could be deemed personal data under the data protection laws of Singapore, India, the US, and the UK, even when encrypted, which would potentially trigger cross-border data transfer or data localization requirements.

- **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 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).

[1] https://fpf.org/wp-content/uploads/2024/09/FPF-Data-Clean-Rooms-Discussion-Sept-2024.pdf at 12
[2] Preventing Financial Fraud Across Different Jurisdictions with Secure Data Collaborations. Infocomm Media Development Authority. PET Sandbox - Mastercard Case Study. Accessed November 2024. https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--mastercard.pdf

- **India**: 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 PET solution would enable disclosures of SPDI to third parties (even cross-border). There are no general data localization requirements under Indian law. However, data localization requirements are specific to the payments sector, laid down in the Reserve Bank of India's ("RBI") Storage of Payment System Data directive. This requires Mastercard (and any bank licensed in India) to store data relating to payment systems in servers or systems only in India. The RBI's FAQs to the directive further clarify that there is no bar on the processing of payment transactions outside India. Still, the data must be deleted from the systems abroad no later than one business day or 24 hours from payment processing (whichever is earlier). 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 PET, 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.

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

- **UK:** Mastercard Europe Services Limited has binding corporate rules ("BCRs") in place, which have been authorized 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 must enter into an additional agreement. Irrespective of the transfer mechanism used, Mastercard must perform a transfer risk assessment. In the UK, the ICO has recognized the use of the technology of the solution to provide "enhanced protection" in circumstances where risk is identified.

Data protection requirements must also be taken into account when considering the feasibility of this FHE solution, including the legal basis for processing personal data, the permissibility of sharing information with third parties for the inquiring entity or the source entity, and individuals' rights under data protection laws to access and correct data collected by the inquiring entity.

- **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 of preventing illegal activities such as financial crime.

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

- **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 fraud prevention, even if the information is not encrypted.

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

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

- **Singapore:** The Banking Act prohibits disclosure of ‘Customer Information’ (CI). If the outputs (True/False) to the query run on encrypted IBANs inadvertently divulge a (non-public) relationship between the customer and the bank, that would likely constitute a 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.

- **India:** The solution reduces the volume of potentially confidential information being shared in 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 bank's interest.

- **US:** The solution does not materially influence Mastercard's compliance with confidentiality restrictions. The GLBA permits sharing non-public personal information with both affiliated and non-affiliated entities to protect against fraud.

- **UK:** The solution would not avoid a duty of confidentiality, and disclosures would need the individual's authorization. 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.

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

Current Adoption Status:
This FHE solution was deployed as a proof of concept, as part of a regulatory sandbox pilot hosted by the Singapore IMDA. The Singapore IMDA write-up of the case is available online.

Benefits of PET Implementation

Privacy Benefits:
The primary privacy benefit of FHE in this case is that a querying entity can get information about a given IBAN without actually exposing the underlying identifier. As a result, individuals who are data subjects do not have their identifiers scattered worldwide. More importantly, the querying entity does not raise suspicion by inquiring. Because the IBAN is encrypted, the remote entities cannot see what identifier is being queried.

This represents a significant improvement over existing solutions, which require sharing IBANs. Not only can this result in the above "suspicion-raising/tipping off" risk, but it also opens individuals to any general issues related to data sharing (leakage, failure to delete, security failures, etc.).

Operational Benefits:
While FHE enables straightforward compliance benefits—being able to perform these checks at all—it is slow and challenging to implement at this stage, which limits the additional benefits.

Potential for Broader Use:
Other use cases involving the same key characteristics (situations where data residing in different jurisdictions, and/or with different entities, in which the ability and/or permissibility of transferring data to, or accessing data from, those jurisdictions or entities is limited or otherwise challenging, and in

which the inquiry parameters can be addressed via Boolean outputs) should be further investigated to determine how they can be addressed using this FHE solution or a similar PET.

Economic Benefits:
While high-quality global estimates are scarce or nonexistent, regional credit card-based cross-border fraud estimates are available. For example, the European Central Bank estimated that "most card fraud (71% of total value in the first half of 2023)... involved cross-border transactions," which amounted to just over €600 million.

Societal Benefits:
This kind of fraud check can potentially make a significant social impact, primarily by reducing the prevalence of cross-border fraud cases.

Risk and Ethical Analysis

Ethical Considerations:
The design and implementation of FHE in this use case are expressly focused on managing the negative impacts on individuals or organizations that could come from more traditional data-linking methods. For example, using the described system, a transaction could be identified as potentially fraudulent without sharing additional information such as where the fraud flag came from. This means that while a transaction might fail, it would be impossible for the network operator to send information about the transactor to law enforcement authorities. While, in general, it might be advantageous to do so, the specific implementation of FHE here effectively limits the information to ONLY that which is required to conduct the task at hand, baking in purpose limitations to the activity.

Trade-offs:
The incorporation of FHE enforces a purpose limitation on the fraud checks, increases user privacy, and mitigates possible biased investigations, but in doing so, carries an inherent lack of flexibility, with each new use case requiring bespoke development and support.

Privacy Risks:
The privacy risk in this use case is low. The main risk arises from multiple jurisdictions collecting linkable data. Although the data is designed to remain encrypted and not linked in plaintext, the concern is the unintentional leakage of fraud risk flags once decrypted by the querying entity. This risk is likely low, as the data would exist regardless. Moreover, the involved parties are strongly motivated to secure the data due to legal, financial, and reputational considerations. A further risk is the lack of explainability of decision-making when it comes to decisions that impact individuals (e.g., decisions to reject certain transactions with an individual would not be explained to that individual), giving the individual no recourse to contest such decisions and/or correct any errors in the underlying data.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005

info@fpf.org | FPF.ORG