PMPG
Payments Market Practice Group

Payments Fraud Contact Database

In the year 2018 the PMPG published version 2.0 of its influential "*Market Practice Guidelines for the cancellation of suspected fraudulent transactions and handling of compliance/regulatory inquiries*". This paper not only received positive feedback in the community but was also applauded by regulators as a step in the right direction to identify shared business practices that can strengthen the cyber incident response of the banking community. Under the leadership of the **Committee on Payments and Market Infrastructures (CPMI**), central banks have issued their own recommendations on how the community should look at the end-to-end ecosystem. The CPMI highlights seven specific aspects that the market should implement, three of which are very relevant to our market practice discussion:

- CPMI recommendation # 5: Respond in a timely way to potential fraud
- CPMI recommendation #6: Ongoing education, awareness, and information sharing
- CPMI recommendation #7: Learn, evolve, and coordinate

These three recommendations require a community response and engagement and are ideally suited for discussion in industry groups such as the PMPG. Following this call to action the PMPG published a second industry recommendation in its Fraud Mitigation series, titled "*Recovery of suspected fraudulent transactions*" which promotes certain practices that might aid in the recovery of funds in the case that the cancellation of a suspected fraudulent transaction is not successful. Following the publication of this paper the CPMI met again with SWIFT and the PMPG in the fall of 2019 and encouraged them to continue their engagement and focus on how the response to fraud can be responded to in a more timely manner.

SWIFT and the PMPG identified improved fraud contact sharing as an area of common interest that can leverage the existing infrastructure created through the SWIFT Customer Security Programme[1](CSP).

Account takeover, business email compromise and other scams continue to increase. The PMPG has been at the forefront to work through processes and procedures on how the industry can respond more effectively in stopping fraudulent payments and blocking access to the proceeds from fraudulent payments. In our previous papers have pointed out that the speed of action matters greatly. While we have provided guidance on how to prioritize payment recalls of

[1] https://www.swift.com/myswift/customer-security-programme-csp

fraudulently initiated transactions, one aspect that we still need to address is how banks can improve the coordination with each other. Despite all available technical solutions, it matters in many cases if you can call the operations area in another bank and alert them about a fraudulent wire. While large banks have contacts available, many smaller institutions lack access to this information.

The goal of this initiative is to support the creation and maintenance of a central repository that the industry can access to look up fraud contact information at another institution.

Concept

The key requirements for the directory are that information has to be easy to collect, needs to be accessible, conform to data privacy requirements, and should fit into an existing maintenance process. This last requirement is met by the annual SWIFT CSP attestation process, which already requires the disclosure of information security contacts.

Data to be collected

Initially we suggest that following information should be collected:

- Organization Name* (should follow CSP convention)
- Fraud Contact Group Name
- Group Email* (Use of a generic name/email address recommended)[2]
- Group Phone Number
- Individual Contact Name*
- Individual Phone Number*
- Operating Hours* (Best practice will be 24x7 availability)

(* Mandatory elements)

Release of this data to counterparties should be based on an explicit consent as part of the annual SWIFT CSP attestation process.

SWIFT should make the contact list available via mySWIFT/SWIFT KYC tool. The contacts details should be exportable by participating SWIFT CSP users. Only banks that publish their details in the fraud directory should be able to access the fraud contact details

By disclosing the contact information, the organization should be able to commit to monitoring and actioning the inquiries sent to their designated contact address, and to ensure that contact information is updated annually in line with CSP requirements.

[2] Use of a generic name should make it easier to meet data privacy requirements. As a group email we can recommend to use a common prefix such as: InterbankFraud@domain (Example: InterbankFraud@bank.com)

As a recommended practice the contacting organization should submit a cancellation request following the PMPG market practice guideline[3] or use SWIFT gSRP as soon as the fraudulent transaction is identified. The contacted organization should be able to respond to (not just acknowledge) an inquiry within 30 minutes of receipt; ensure a SWIFT E&I response is provided within 2 hours; update contact details immediately when they change (or at least within 48 hours).

Maybe we can add a flag if an organization is able to support this practice.

Use Cases for Fraud Contact Database (draft)

Scenario: A bank has instructed a payment via SWIFT and discovers that the transfer has not been authorized. The fraud could be internal; due to a system take-over through malware or a customer of the bank could have fallen victim to a fraud.

The bank should implement the following best practices:

- Sign up for Stop & Recall
- Use the gpi tracker to determine the status of the payment

Step 1: Initiate a cancellation via Stop & Recall as soon as the fraud has been reported. If the recall cannot be confirmed, then

Step 2: Check the gpi tracker if the bene bank has credited the account of the beneficiary and view the data and time of the credit, if the credit is within the last 24h and the payment is above USD 10,000 or equivalent local ccy, then

Step 3: Look up the fraud contact details using the bene banks BIC code in the fraud contact database. The details in the database will show a general contact number that can be called or an email address.

Step 4: When contacting the beneficiary bank please quote the case number, reference number from your cancellation message), payment amount and beneficiary account number.

Step 5: The bank that is being contacted should locate the cancellation message based on the information provided and either return the payment if it has not been credited yet to the beneficiary or place a hold on the account that covers the amount of the disputed funds, if permissible under local law.

Step 6: Both banks should follow the guidelines in the **Recovery of suspected fraudulent transactions** Market Practice Guideline (https://www.swift.com/swift-resource/229376/download)

[3] https://www.swift.com/file/64546/download?token=5KccwN8c