Recovery of suspected fraudulent transactions

Market Practice Guidelines – Fraud Mitigation Part II

(Version 1.0)

The Payments Market Practice Group (PMPG) is an independent body of payments subject matter experts from Asia Pacific, EMEA and North America. The mission of the PMPG is to:

- Take stock of payments market practices across regions
- Discuss, explain, and document market practice issues, including possible commercial impact
- Recommend market practices, covering end-to-end transactions
- Propose best practice, business responsibilities and rules, message flows, consistent implementation of ISO messaging standards and exception definitions
- Ensure publication of recommended best practices
- Recommend payments market practices in response to changing compliance requirements

The PMPG provides a truly global forum to drive better market practices, together with correct use of standards, will help in achieving full STP and improved customer service.

Introduction

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". The 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[1] 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 has decided to recommend certain practices that might aid in the recovery of funds in the case that the cancellation of a suspected fraudulent transaction is not successful and that funds have been credited to the creditor's account.

[1] CPMI: Reducing the risk of wholesale payments fraud related to endpoint security, May 2018: https://www.bis.org/cpmi/publ/d178.pdf, last accessed June 17, 2019

Background

The purpose of this document is to establish market practice guidelines for the communities to aid each other in the recovery of funds from suspected fraudulent cross-border payments. To be more precise we propose the following scenarios:

- **Fraudulent initiation of a transaction:** Debtor or debtor agent did not intend to instruct payment to the specific creditor. This could be due to a business email compromise, cyber-attack or invoice fraud.
- **Fraudulent business activity:** Debtor or debtor agent intended to instruct the payment to the specific creditor but later discovered out that the underlying justification for the payment was a scam (romance, inheritance, investment fraud etc.)

In this paper, we are focused on the recall of funds in the first scenario. The second scenario is by far more complex and may involve multi-year fraudulent business activity.

The specific scenario that this paper tries to address is as follows: An allegedly fraudulent transfer[2] has been credited to the creditor's account. The debtor or the debtor's agent has noticed that funds were moved due to some nefarious action. A cancellation is generated claiming fraud. Two possible scenarios can emerge at this time:

a) All, or at least most, of the funds are in the creditor's account when the creditor agent received the cancellation request
b) All, or most of the money has been moved by the creditor through one or multiple transfers to other agents.

The question that the PMPG members asked themselves was: What support can the original creditor agent offer in the recovery of funds? Can cancelation messages be sent to the creditor agent of the new transfers? Fraudsters are getting more sophisticated in using one or multiple mule accounts, taking accounts over and layering funds into the financial system. What alerts or notifications should be provided to other banks?

Timely action is of the essence in this situation as research has shown that funds normally will be moved within 72hours or less. The faster the bank chain can react, the greater the likelihood of recovery. While the SWIFT gpi stop and recall service improves the cancellation of funds in transit we need to look at options when alleged fraudulent funds have been credited to the creditor's account.

[2] Fraudulently initiated

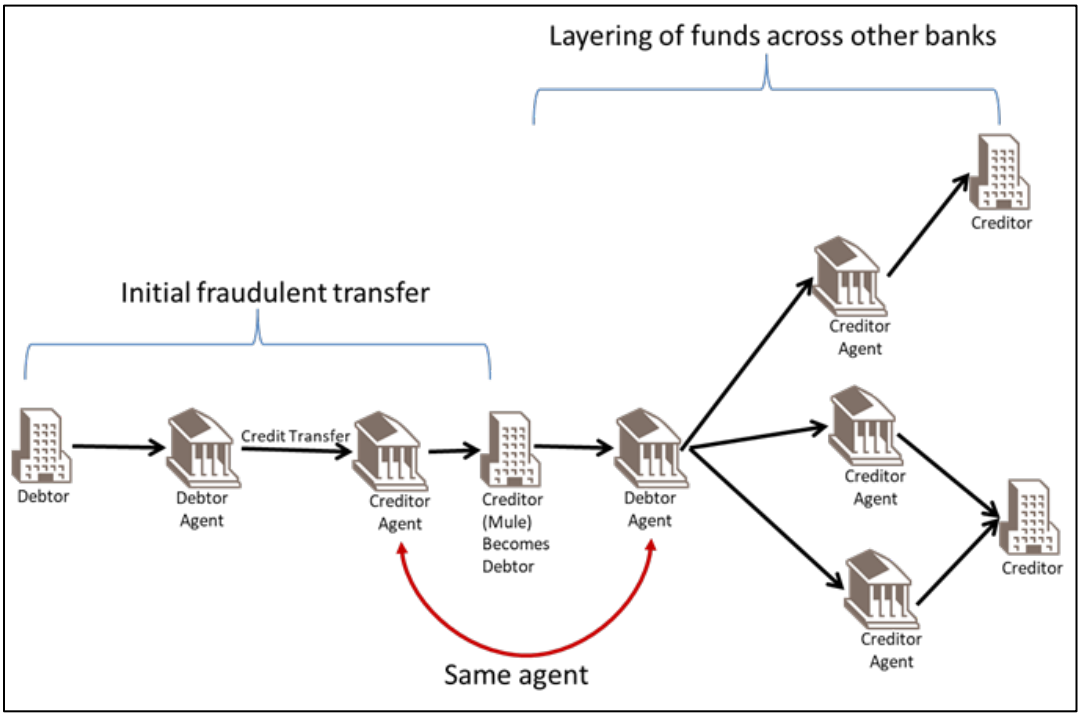

Figure 1: Layering of payments to obfuscate the perpetrators

The practices outlined in this document try to balance the responsibilities of the different parties in order to make it more difficult to extract funds obtained through fraudulent transactions out of the banking system:

- The debtor needs to take precautions and safe guards before initiating a transaction to ensure that the creditor and creditor account details are correct.
- The debtor agent should screen payment transactions for unusual behavior and secure their own systems as outlined in the SWIFT CSP program[3]. The debtor agent should educate customers to identify business email compromise and scams.
- The creditor agent should have a program in place to identify mule accounts and screen incoming credits for unusual activity.

No single recommendation outlined below will guarantee that funds generated through fraudulent activity will be returned to the debtor but collectively these practices will make it more difficult to extract these fraudulent funds from the banking system

[3] In 2020 the SWIFT CSP will require an external party to validate the attestation.

Market Practice Guidelines

MPG Funds Recovery #1: Follow the business flow and associated recommendations from the previous Market Practice Guidelines

The *Cancellation of suspected fraudulent transactions and handling of compliance/regulatory inquiries* MPG describes the recommended business flow (including message type, structure and codewords) to facilitate the cancellation, response and ultimately return of fraudulently initiated funds. Figure 1 demonstrates this flow, sequencing and where the recommendations in this paper would be applicable.

MPG Funds Recovery #2: File a local police report or lodge information with IC3[4]

In most cases the debtor, as the directly harmed party, will file a report with the local police. The debtor agent should request copies of the police report from the debtor (harmed party) and. if applicable, file a report on the IC3 website[5]. This information should be made available to the creditor agent or if an English version is not available, the debtor agent should confirm the key facts of the police report to the creditor agent. This information can enable the creditor agent to hold the funds and deny the debtor access to the funds for some limited time.

Note

No structured message type exists at this time to submit this information via SWIFT to the creditor agent. Secure email and fax are the only two communication tools currently available. In many cases, direct contact between Financial Crimes or Fraud units will be required. The PMPG is recommending that the community approach SWIFT to enable the easy exchange and management of contact information between banks.

MPG Funds Recovery #3: Use of the BAFT Indemnity letter template

As discussed in the PMPG *Cancellation of suspected fraudulent transactions and handling of compliance/regulatory inquiries* MPG, the debtor agent indicating a willingness to indemnify (if appropriate) in the original cancellation request provides the best opportunity for funds to be held. Similarly, the creditor agent indicating a need for indemnification in their initial response to the cancellation, request provides the best opportunity to expedite the process.

[4] https://complaint.ic3.gov/default.aspx
[5] If the currency of the fraudulent payment is USD or involves an agent or party located in the US

To further reduce friction in the process, we recognise the need to agree on a standard indemnity template that, while unable to be perfect for all stakeholders in the global payment community given the environment of multiple legal jurisdictions and incongruous internal policy, is accepted as a reasonable foundation document with which we can all work. In that context, the PMPG recommends the use of the BAFT indemnity letter template[6]. The indemnity can either be exchanged directly between the creditor agent and the debtor agent or via an intermediary[7].

As mentioned in the previous MPG, a standard mechanism to exchange documentation such as an indemnity and local contact information with the various FIs involved, will also benefit the process.

MPG Funds Recovery #4: Holding of funds

After receiving a cancellation request containing the FRAD codeword via SWIFT the creditor agent should place an amount hold on the creditor's account that covers the recalled amount. The hold should be in place for *three business days* to allow the debtor or debtor agent to submit the relevant police reports to the creditor agent.

After receiving the police reports, the creditor agent should restrict access to the funds for an additional 21 business days to allow the debtor agent to submit the LOI or file a claim in the local courts.

Note

In many cases, the creditor agent's hands are tied due to local laws or regulations. The PMPG would like to encourage local communities to reach out to the regulators and legislative bodies to allow creditor agents to restrict the creditor's access to the funds in the case sufficient evidence is provided (e.g. via the police report on #2 above) that the credited funds are allegedly sourced through illegal activity. The creditor agent should be permitted to restrict access to the funds for a limited period of time ("cool off period") to allow the debtor or debtor agent to submit the letter of indemnity (see #3 above) to the creditor agent or file a legal claim against the creditor in the local courts. During this cool-off period the creditor agent should be held harmless as acting in good faith.

MPG Funds Recovery #5: Educate account owners

Account servicing institutions should educate account owners about the proper use of accounts

[6] As local legal requirements vary each community will need to decide if the BAFT indemnity letter is acceptable from a local legal perspective.

[7] Risk appetite will determine if the intermediary is supporting a back to back indemnity

and advise them not to accept funds on behalf of third parties. For example education programs on the proper use and handling of debit, credit cards and checks are quite common for consumer payment instruments and educating account holders on the dangers of acting as a money mule should be included as well. Specifically account owners should be educated on:

- Refusing to receive money on behalf of someone else.
- Not believing attractive offers/commissions that appear to be too good to be true; refusing to receive unauthorized payments
- Informing their bank immediately should their account be credited with funds not due to them
- Understanding the implications and dangers of being complicit in money laundering

Observations and Recommendations

The PMPG is not a regulatory body and cannot enforce any of the guidelines. It can only point out practices which, when followed properly, are beneficial to the payments community.

Beyond the guidelines stated above, the community can use recommendations the below to further improve the handling of fraud and compliance inquiries:

Tracking of downstream payments

The PMPG would like to encourage SWIFT to explore how options and explore how SWIFT gpi can be used to track payments that were initiated by a debtor that was also the recipient of a fraudulently initiated transfer. As this is a sensitive topic consideration should be given to the following:

- Visualization of the value of each transaction, perhaps without displaying the actual amount.
- How much to display about the creditor or creditor agent on the disbursed funds
- What information is important about the disbursed funds, such as UTER, country, etc.

Fraud database

Community solutions such as FS-ISAC should be leveraged to communicate non-cyber incident related fraud schemes. The PMPG would like to encourage SWIFT to explore how the current cyber security incident sharing arrangement can be expanded to cover account takeover and fraud and mule accounts.

An industry wide fraud database can also be integrated into the SWIFT gpi pre-validation process or the SWIFT Payment Control Tool.

Expansion of regional indemnity templates

The concept to support different indemnity templates to cater to regional needs can be further build out by BAFT and it should be explored if additional regional variants should be added.

Glossary of Terms

Creditor: Party to which an amount of money is due. In the current MT message implementation, this is the beneficiary

Creditor Agent: Financial Institution servicing an account for the creditor (beneficiary). In the current MT message implementation this is referred to as the Beneficiary Bank or Account With Bank

Debtor Agent: Financial Institution servicing an account for the debtor (ordering party). In the current MT message implementation this is referred to as the Ordering Bank

Debtor: Party that owes money to the creditor. In the current MT message implementation, this is the Ordering Party