Information paper

Mitigating fraud risk through strengthened payment operations

Recent cybercrime events have demonstrated the important role that strong reconciliation and response processes play in detecting fraud that has been perpetrated through back-office systems.

While many banks rigorously check confirmations and statements, others do not realise that these practices are the cornerstone of payment operations and can help them avoid falling victim to fraud.

Others may be unaware of how best to respond when fraudulent or suspect transactions have been sent.

The evolving character of cyber threats has changed the fraud landscape considerably. Institutions are re-evaluating their back-office systems and controls, and are reviewing the approach taken to fraud detection and prevention. The importance of strengthening controls was recently underlined by the launch of SWIFT's Customer Security Programme (CSP), which aims to help financial institutions bolster their IT fraud prevention and detection controls and procedures and emphasises the requirement for customers to report fraud incidents.

In this climate, seemingly old-fashioned operational processes which aim to maintain the hygiene of payment operation systems and processes are often forgotten. However, these are the foundation on which other controls should be built.

One area which is frequently overlooked is the need to examine message confirmations and end-of-day statements. Payment confirmations should be generated whenever a transaction is made. Checking that these confirmations reflect the relevant transactions is a simple process which can help banks to avoid the risk of falling victim to fraud. Similarly, end-of-day statements should be checked for discrepancies.

If a fraud or suspected fraud is identified, following proper market practice for cancellations can increase the likelihood of success, reduce the impact of any fraud that does take place and increase the likelihood and speed of recovery of funds.

These processes should be part of any institution's toolbox when it comes to fraud prevention. However, many banks do not check confirmations and statements as a matter of course, or are reliant on their correspondents' record keeping. Others are unaware of the specific process involved in cancelling a suspected fraudulent transaction.

By improving the hygiene of operational processes, banks may be able to identify fraudulent transactions more quickly and increase the likelihood that funds can be recovered if fraudulent payments are made. This paper explains the processes that banks should have in place to check settlement instructions and to take action to cancel fraudulent messages.

Checking settlement instructions

When a consumer makes a purchase, they instinctively look at their receipt to check that the transaction is correct. Banks should adopt the same approach to check their confirmations and statements, such as MT 900, MT 910, MT 940 and MT 950 messages. Checking can be carried out either automatically or manually. What is important is to have a review process in place whereby banks check that the confirmations and statements match the transactions which should have occurred on the accounts.

Checking confirmations

When a payment is sent, banks usually receive confirmations, such as confirmation of debit (MT 900) and confirmation of credit (MT 910) messages. These messages are received as soon as a payment has been made, notifying the account owner of entries that have been debited or credited to their account.

It is good practice to check that the messages match the transaction which has been made, but in practice some banks do not perform this additional check. Some banks may simply assume that the information provided by their correspondents is accurate, or as confirmations are optional counterparts may decide not to send them. However, the use of confirmations is good practice and banks should encourage their counterparts to provide them.

Checking statements

Statement messages, such as MT 940 / MT 950, should also be checked to ensure that they align with expectations and in order to highlight any discrepancies. These are end-of-day messages which provide balance information and details of the transaction activity for the account owner. Statements provide a record of SWIFT-related transactions as well as transactions which may not have been sent over SWIFT, such as an interest payment on an account.

It is important to validate statements in order to confirm that the amounts and balances recorded meet the bank's expectations. Banks should therefore have a daily reconciliation process in place whereby all items in the statement are matched against the institution's accounting records. Again, any discrepancies need to be accounted for. These could suggest fraudulent activity, or unusual activity indicative of other business, operational or financial crime-related risks.

If additional intraday information is required, intraday transactions and balance reports can be requested from counterparts using an MT 920.

Changing payment instructions

On a related note, free format messages such as MT 199 should not be used to manipulate or change payment instructions. Such messages are used for communication between institutions, but should not be used as a vehicle to manipulate payments as it can lead to issues where reconciliation is concerned. Regulatory requirements mean that this practice is increasingly unacceptable for many institutions and in many jurisdictions. Instead, institutions should amend the original instructions by cancelling and recalling or by sending payment adjustments.

Cancelling instructions

If fraudulent or suspicious activities are detected, appropriate action needs to be taken immediately. With the right processes in place, banks may have an opportunity to minimise fraud loss or increase the likelihood that funds can be recovered.

When a problem arises with a payment, banks can send a cancellation message.

This message takes one form when a straightforward error is identified – but banks are often unaware that an additional flag should be included in the message when the message being cancelled is fraudulent. This flag indicates to the recipient that the cancellation is associated with fraud and should be prioritised and pushed to the top of the processing queue, with appropriate action taken to hold or freeze funds before settlement completion.

The appropriate message to request cancellation of a payment instruction is the MT n92, where 'n' depends on the category of the original message. So to cancel an MT 103, an MT 192 is used; for an MT 202, an MT 292 is used etc.

To request cancellation of a suspected fraudulent payment instruction, field 79 of the MT n92 should be used with the code-word /FRAD/.

Checking statements and confirmations

Opening Balance

MT 950 - statement
MT 940 - customer statement

Movement Confirmation

MT 900 - debit confirmation
MT 910 - credit confirmation

By sending an MT 920 request, these can be complemented with:
- MT 942 - interim transaction report
- MT 941 - balance report

Closing Balance

MT 950 - statement
MT 940 - customer statement

Cancellation example

A bank might send the following MT 103 Single Customer Credit Transfer which is subsequently discovered to be fraudulent:

From: Sender BIC
103
To: Receiver BIC

:20:1234567890
:23B:CRED
:32A:160910EUR800000,00
:50F:/942267890
1/FRANZ HOLZAPFEL GMBH
2/GELBSTRASSE, 13
3/AT/VIENNA
:57A:BANKGB22
:59:/9876
A. FRAUDSTER
1, CROOKED STREET
LONDON
:71A:SHA

The following MT 192 should be sent as soon as possible to the recipient of the MT 103:

From: Sender BIC
192
To: Receiver BIC

:20:ABC123
:21:1234567890
:11S:103
160809
:79:/FRAD/
:20:1234567890
:23B:CRED
:32A:160810EUR800000,00
:50F:/942267890
1/FRANZ HOLZAPFEL GMBH
2/GELBSTRASSE, 13
3/AT/VIENNA
:57A:BANKGB22
:59:/9876
A. FRAUDSTER
1, CROOKED STREET
LONDON
:71A:SHA

- Field 20 of the message believed fraudulent
- The message was an MT 103...
- ...sent on 9th August 2016
- Cancellation request relates to a fraud
- Copy of the original message details

If the original message is not available in FIN format, a full description should be provided as follows:

From: Sender BIC
192
To: Receiver BIC

:20:ABC123
:21:1234567890
:11S:103
160809
:79:/FRAD/
Payment of EUR 800000,00
value dated August 10.
Ordering Customer
/942267890
1/FRANZ HOLZAPFEL GMBH
2/GELBSTRASSE, 13
3/AT/VIENNA
Beneficiary Bank
BANKGB22
Beneficiary Customer
/9876
A. FRAUDSTER
1, CROOKED STREET
LONDON

- Field 20 of the message believed fraudulent
- The message was an MT 103...
- ...sent on 9th August 2016
- Cancellation request relates to a fraud
- Description of the transaction including beneficiary, beneficiary bank, and account

Advice for recipients

The recipients of cancellation requests can identify requests related to fraud from the /FRAD/ code word that appears in field 79.

The successful execution, or failure to execute, of a cancellation request should be advised to the requestor using an MT n96 (where 'n' corresponds to the category of the cancellation request received). For example, if the cancellation shown in the previous section were executed successfully, the following MT 196 message would be returned:

From:Sender BIC
196
To:Receiver BIC
:20:XYZ789
:21:ABC123
:76:CANCELLED
:11R:103
160809

- Field 20 of the MT 192 received
- Indicates MT 103 successfully cancelled

It is important to note that if the transactions in question are a sequence of serial payments, the recipient may, in turn, need to send additional cancellations to counterparts in the payment chain.

If the cancellation request cannot be executed, for example because the request was received too late, an MT 196 may be returned specifying special code /12/ in field 76 with an appropriate narrative:

From:Sender BIC
196
To:Receiver BIC
:20:XYZ789
:21:ABC123
:76:/12/payment already processed
:11R:103
160809

- Field 20 of the MT 192 received
- /12/ stop instructions not acceptable

It is recognised that not all institutions support n96 'answer' messages. Where this is the case n99 may be considered as an alternative, using the guiding principles above.

Conclusion

With fraud prevention high on the agenda, it is important that banks use all available tools to monitor payment patterns.

Checking confirmations and end-of-day statements is a simple step which can significantly reduce the risk that a financial institution will fall victim to fraud. Meanwhile, using the correct cancellation code can increase the likelihood that a transaction will be stopped successfully. Banks are required to promptly report fraudulent activity to SWIFT Support.

Senior managers and fraud professionals should ensure that these sound business practices are in place.

Best Practice

By adopting the following practices, financial institutions can increase the likelihood that fraudulent activity will be detected and, potentially, reversed:

- Encourage counterparts to provide confirmations if they are not already doing so.
- Check that confirmations and statements are as expected.
- Avoid using free format messages to change payment instructions.
- Use the appropriate codes when sending cancellation messages.
- Report any incidents to SWIFT Support.

For further information on this topic, banks can consult the relevant SWIFT message standards, available in the User Handbook on www.swift.com

SWIFT Customer Security Programme

Combating fraud is a challenge for the whole industry – there are no quick fixes. The threat landscape adapts and evolves by the day, and both SWIFT and its customers have to remain vigilant and proactive over the long term. While customers are responsible for protecting their own environments, SWIFT's Customer Security Programme (CSP) has been established to support customers in the fight against cyber-attacks. This programme addresses three key aspects of your business and your relationships, enabling you to take action with the support of SWIFT's programme.

1. You

Securing your own local environment is the most important action you can take. Securing the physical set-up of your local SWIFT-related infrastructure and putting in place the right people, policies and practices, are critical to avoiding cyber-related fraud.

What you can do

Take all preventive measures to secure your local environment; sign up to SWIFT's Security Notification Service; stay up to date with SWIFT's latest security updates; get ready to adopt our new security requirements.

2. Your counterparts

Companies do not operate in a vacuum and all financial institutions are part of a broader ecosystem. Even with strong security measures in place, attackers are very sophisticated and you need to assume that the worst may happen. That's why it is also vital to manage security risk in your interactions and relationships with your counterparties – which fall into two main areas:

If you are breached

Strong detection measures need to be put in place to increase the chances of stopping fraud in case your environment is breached. To support smaller institutions in particular, SWIFT has launched new anti-fraud reporting tools to provide customers with activity reports which provide an original record of their transaction data over SWIFT. These Daily Validation Reports offer both a secondary check on transactions to prevent and detect fraud and a focused review of large or unusual flows. They are available as a back-up to customers even if their own environment has been compromised and their records altered.

If your counterparty is breached

You also need to prepare for the possibility that one of your counterparties has been breached, and that you may receive suspicious traffic over SWIFT originating elsewhere. A basic starting point is to check that you are only doing business with trusted counterparties. SWIFT's Relationship Management Application (RMA) supports customers by enabling them to control access through RMA tools. Market practice also has an important role to play in handling your counterparty relationships. SWIFT is facilitating discussions with banks to develop a common understanding between sending and receiving parties of the warning signs that should lead to payments being investigated, and of how suspicious payments should be stopped.

What you can do

Put in place detection measures; 'clean-up' your RMA relationships; engage with us on market practice.

3. Your community

The financial industry is truly global, and so are the cyber challenges it faces. What happens to one company in one location can easily be replicated elsewhere in the world.

If the worst happens, or you suspect something is wrong, it is vital that you share all relevant information and tell us there is a problem – which is part of your obligation to SWIFT as a user.

In cases of suspected customer fraud, it is important to act fast and take decisions in real time. That's why SWIFT also reserves the right to temporarily block or inhibit such customer's outgoing messaging flows if fraud is strongly suspected and we have been unable to directly contact the customer in question in a reasonable timeframe.

What you can do

Inform SWIFT if you suspect that you have been compromised; sign up to our security notification service and act upon the information; provide SWIFT with the contact details of your company's CISO for incident escalation; install all mandatory updates from SWIFT within the prescribed timeframes.

Summary

By focusing action on supporting your efforts, your counterparty relationships, and your community, SWIFT's CSP is already making a strong impact on preventing, detecting and responding to fraud and reinforcing the security of global banking. The fraud threat is adaptive, so the tools and controls introduced under the CSP will continue evolving, and we are committed to working over the long term to achieve the objectives of the programme.

This is the first part of a journey which involves SWIFT and its community of customers, regulators, overseers and third parties to collectively work together to fight against cyberattacks.

For further information visit:
www.swift.com/csp

About SWIFT

For more than 40 years, SWIFT has helped the industry address many of its biggest challenges. As a global member-owned cooperative and the world's leading provider of secure financial messaging services, we enable more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, relentlessly pursue operational excellence, and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. We also bring the financial community together to work collaboratively to shape market practice, define standards and debate issues of mutual interest.

SWIFT users face unprecedented pressure to comply with regulatory obligations, particularly in relation to the detection and prevention of financial crime. In response, we have developed community-based solutions that address effectiveness and efficiency and reduce the effort and cost of compliance activities. Our Compliance Services unit manages a growing portfolio of financial crime compliance services in the areas of Sanctions, KYC and CTF/AML.

SWIFT's Customer Security Programme, which launched in June 2016, is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts. The programme will clearly define an operational and security baseline that customers must meet to protect the processing and handling of their SWIFT transactions.

SWIFT will also continue to enhance its own products and services to provide customers with additional protection and detection mechanisms, and in turn help customers to meet these baselines.

swiftcommunity

company/SWIFT

Trademarks

Disclaimer

Copyright

57242 - December 2016