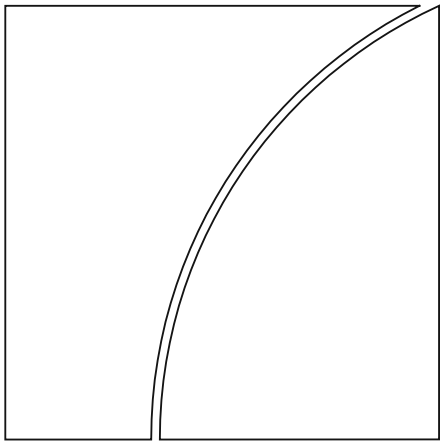
Committee on Payments and Market Infrastructures

Discussion note



Reducing the risk of wholesale payments fraud related to endpoint security

September 2017

BANK FOR INTERNATIONAL SETTLEMENTS

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-091-8 (online)

Table of contents

1. Introduction

In September 2016, responding to the increasing threat of wholesale payments fraud, the Committee on Payments and Market Infrastructures (CPMI) announced the establishment of a task force (TF) to look into the security of wholesale payments that involve banks, financial market infrastructures (FMIs) and other financial institutions.[1] This TF has developed a proposal for a strategy to reduce the risk of wholesale payments fraud related to endpoint security (hereinafter wholesale payments fraud). The strategy's primary aim is to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud and, in doing so, support financial stability. The purpose of this note is to present the proposal and to seek input from relevant stakeholders.

2. Wholesale payment ecosystem and endpoints

A safe, reliable, secure and efficient wholesale payment system is an essential component of a well functioning financial system. A wholesale payment system is connected by a supporting messaging network with banks, FMIs and other financial institutions and service providers, forming a complex ecosystem. Central banks have long had a special interest in the wholesale payment ecosystem, both as owners and operators of wholesale payment systems and as overseers of these systems. Further, central banks use a wholesale payment system for their monetary policy implementation and provision of liquidity to maintain financial stability.

Fraud in the wholesale payment ecosystem is becoming increasingly sophisticated, and recent examples have shown that weaknesses in security at one endpoint in the ecosystem can be exploited to commit payments fraud. For the purposes of this note, an endpoint in the wholesale payment ecosystem is defined to be a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem, such as between a payment system and a messaging network, between a messaging network and a participant in the network, or between a payment system and a participant in the system.[2]

3. Risk of wholesale payments fraud and need for a holistic approach and coordination

While wholesale payments fraud can cause material risks to individual financial institutions, it may also have a broader systemic impact on a wholesale payment system, its ecosystem and the broader economy. Given the interconnectedness of various stakeholders in the wholesale payment ecosystem, fraud may not only result in financial losses and reputational risk in the compromised endpoint, but, in an extreme case and in the absence of appropriate arrangements within the ecosystem for preventing, detecting, responding to and communicating about fraud, may undermine confidence in the integrity of the entire system. If participants have concerns about the security of the payments network, their own security or the security of other participants, each of them may implement additional controls before releasing

[1] See www.bis.org/press/p160916.htm.

[2] In physical terms, an endpoint may include devices connecting to one or more parties in the ecosystem. Such devices include mobile devices, laptop or desktop PCs and hardware such as servers. Devices at endpoints may or may not be controlled directly by the operator of a payment system or messaging network.

payments or may limit or halt payment instruction processing. When confidence in the integrity of the entire system has been lost, such individual precautionary actions could, in aggregate, create significant gridlock in payment processing, reduce overall liquidity in the financial markets and potentially cause a build-up of unsettled positions and bilateral credit exposures among financial institutions. These actions could ultimately impede economic activity and financial stability.

In addressing the potential risk of wholesale payments fraud to the financial system and broader economy, a wholesale payment ecosystem faces distinct challenges. First, wholesale payments fraud is becoming increasingly sophisticated and is expected to evolve further. Second, wholesale payments are typically large-value, immediate and final, which may make them more susceptible to be targeted for fraud in the first place and increase complexities in addressing the risk. Third, operators of payment systems and messaging networks alone cannot verify and control every aspect of endpoint security, and need to rely on those who control the endpoints or are closer to them to ensure that appropriate controls are in place and operating effectively. Given the interconnectedness of financial networks, the efforts of single parties may not achieve the expected benefit unless other connected parties do the same. Lastly, each participant of payment systems and messaging networks has inherent incentives to guard against the risk of wholesale payments fraud to avoid potentially large financial losses and reputational damage and should be expected to bear primary responsibility for taking necessary action. However, the broader economic impacts and social costs as described above may not be sufficiently anticipated and internalised by individual parties, resulting in an insufficient level of action and investment to reduce the risk of wholesale payments fraud.

All these factors point to the criticality of better understanding the full range of risks and the need for better coordination. It is vital that all relevant stakeholders, including operators of payment systems and messaging networks, their participants and relevant authorities, take a holistic and more coordinated approach to guarding against the loss of confidence in the integrity of the wholesale payment ecosystem as a whole.

4. Preliminary findings by the TF

The TF conducted a preliminary stocktaking of current expectations[3] and requirements[4] in CPMI member jurisdictions for preventing, detecting, responding to and communicating about fraud in wholesale payments related to endpoint security (see Annex 1 for a description of the analytical framework developed for the exercise). The preliminary stocktaking revealed knowledge gaps, inconsistencies in approaches and potentially important opportunities to strengthen the overall endpoint security of the wholesale payment ecosystem to reduce the risk of fraud. For example:

- Many payment system operators do not have expectations or requirements in place for senders or receivers of payment messages to prevent or detect fraud related to endpoint security.
- For those operators that do have in place expectations or requirements for prevention or detection, many do not require confirmation of adherence to those requirements or conduct assessments of adherence.

[3] Examples of current expectations include industry best/good practices, recommendations, codes of conduct and self-declarations.

[4] Examples of requirements include rules, procedures and other contractual obligations, and regulatory and/or legal requirements.

- In terms of the immediate response to detected fraud, there are limited expectations or requirements for senders and receivers to inform each other or law enforcement of attempted or actual fraud.

Based on those findings, TF members engaged in dialogue with the industry. The preliminary stocktaking and industry dialogue proved to be informative and productive, and indicated the value of further CPMI actions.

As an outgrowth of this work, the CPMI developed a strategy to reduce the risk of wholesale payments fraud. The strategy is under development, and a key purpose of this note is to seek input on essential aspects of the strategy. Its primary aim is to encourage and help focus industry efforts to reduce the risk of wholesale payments fraud, taking into consideration a number of important initiatives that are already under way. The analytical approach and terminology used in the note should also promote clarity and consistency amongst the various stakeholders as they advance their efforts to reduce the risk of wholesale payments fraud.

5. Proposed strategy for reducing the risk of wholesale payments fraud related to endpoint security

The strategy is designed to be taken into account by all relevant public and private sector stakeholders in reducing the risk of wholesale payments fraud, including operators of payment systems and messaging networks, their participants and the respective supervisors, regulators and overseers of these operators and participants.[5] The strategy is composed of seven elements. These elements are designed to work holistically to address all areas relevant to preventing, detecting, responding to and communicating about fraud. These elements describe what should be done at a high level, recognising the need for flexibility when approaching each element. Such flexibility will allow payment systems and messaging networks to adopt and operationalise the elements in accordance with their unique architecture and processes, while taking into account changes to their risk environment and the evolution of risk management technologies and tools. The CPMI is seeking feedback on the efficacy, completeness and relevance of the elements of the strategy. The seven elements of the strategy are:

1. **Identify and understand the range of risks.** The operator and participants of a payment system and those of a messaging network should identify and understand the risks related to endpoint security that they face individually and collectively, including risks related to the potential loss of confidence in the integrity of the payment system or messaging network itself.

2. **Establish endpoint requirements.** The operator of a payment system or a messaging network should establish clear endpoint security requirements for its participants as part of its participation requirements. Such requirements should include those for the prevention and detection of fraud, for the immediate response to fraud and, when appropriate, for alerting the broader payments network community to evolving fraud threats. In addition to the requirements established by the operator of a payment system or a messaging network, each participant of the payment system or messaging network should identify and establish its own, supplemental risk-based endpoint security requirements as needed.

[5] The terms "operator(s)" and "participant(s)" throughout this note should be understood to include, where applicable and relevant, any third-party service provider(s) they may rely upon in carrying out their respective functions as operator(s) or participant(s).

3. **Promote adherence.** Based upon the understanding of the risks and the endpoint requirements of a payment system or a messaging network, the operator and participants of the payment system or messaging network should establish processes as necessary to help ensure adherence to their respective endpoint security requirements.

4. **Provide and use information and tools to improve prevention and detection.** To the extent reasonably possible, the operator and participants of a payment system or a messaging network should support the provision and use of information and tools that would enhance their and each other's respective capabilities to prevent and to detect in a timely manner attempted wholesale payments fraud.

5. **Respond in a timely way to potential fraud.** The operator and participants of a payment system or a messaging network should adopt procedures and practices, and deploy sufficient resources, to respond to actual or suspected fraud in a timely manner. This includes, where possible and appropriate, supporting the timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction when detected.

6. **Support ongoing education, awareness and information-sharing.** The operator and participants of a payment system or a messaging network should collaborate to identify and promote the adoption of procedures and practices, and the deployment of sufficient resources, that would support ongoing education, awareness and, to the extent appropriate and legally permissible, information-sharing about evolving endpoint security risks and risk controls.

7. **Learn, evolve and coordinate.** The operator and participants of a payment system or a messaging network should monitor evolving endpoint security risks and risk controls, and review and update their endpoint security requirements, procedures, practices and resources accordingly. In addition, the operators and, to the extent practicable, participants of different payment systems and messaging networks should seek to coordinate approaches for strengthening endpoint security across payment systems and messaging networks in order to obtain potential implementation efficiencies where possible and appropriate. Similarly, supervisors, regulators and overseers of payment systems and messaging network and participants of payment systems and messaging networks should review and update their supervisory/oversight expectations and assessment programmes to reflect the evolving risk mitigation strategies.

It should be noted that although the strategy is relevant for a number of risk management topics that are covered by the 24 principles of CPMI-IOSCO *Principles for financial market infrastructures* (PFMI), the expectations in Annex F of the PFMI ("Oversight expectations applicable to critical service providers") and related guidance, including the CPMI-IOSCO *Guidance on cyber resilience for financial market infrastructures,* the strategy is not intended to replace or supersede them. Nevertheless, since the scope of this strategy complements some of these principles and expectations, the strategy could be taken into account by payment systems and messaging networks as they consider their approaches for observing the principles and expectations, where applicable and appropriate. More generally, the strategy is designed to be taken into account by all relevant public and private sector stakeholders in reducing the risk of wholesale payments fraud, including operators of a payment system or a messaging network, their respective participants and the respective supervisors, regulators and overseers of these operators and participants.

6. Operationalising the strategy

After the consultation on this note, the CPMI plans to develop guidance for each element to inform operators and participants of payment systems and messaging networks, as well as other relevant stakeholders, on how they could approach each of the seven elements. The proposed guidance will be developed by early 2018. The CPMI will continue to engage closely with the industry and other relevant stakeholders as it develops the guidance.

In developing the guidance, the CPMI will be mindful that the risk environment and risk management tools may evolve over time. It will be also mindful that, while payment systems and messaging networks share many commonalities with one another, they vary in several aspects, including the number and diversity of their participants; the volume and nature of the underlying obligations being settled; and the relevant legal, operational and technological structures and constraints under which they may operate. Such variations may have important implications for determining the most appropriate and effective approaches to operationalising the strategy, such as when considering possible options for:

- Promoting adherence to endpoint security requirements.
- Developing/selecting tools that would allow participants to screen or to control their own payment instructions (eg self-imposed restrictions based on specific parameters such as operating hours and days, transaction amounts, counterparties and types of transactions).
- Potentially granting each participant the choice to pre-authorise whether or not it is willing to receive payments from another participant in the payment system or messaging network.
- Developing procedures and practices for responding when an attempted, suspected or actually fraudulent payment is detected, and for responding to a request to take action following such detection.
- Potentially restricting or suspending a participant's access if and when a participant's endpoint security is determined to be deficient.

In the light of these and other possible differences across payment systems and messaging networks, the CPMI would welcome input for developing guidance with appropriate flexibility for approaching each element that takes into account the unique attributes of each payment system and messaging network.

7. Request for comment

Overall strategy and seven elements

The CPMI requests comment and feedback on the overall strategy and its seven elements, including with respect to the efficacy, completeness and relevance of the seven elements of the strategy, and whether any other elements should be added.

Development of guidance

The CPMI is also seeking input that would assist in developing the prospective guidance for taking forward the strategy. It would be particularly helpful if input provided for developing guidance for approaching

each element could address the following aspects, including unique attributes of each payment system and messaging network:

1) Specific challenges and opportunities for approaching each element.

2) Specific suggestions, existing good practices and examples of relevant efforts under way or under consideration that could help advance the strategy.

3) Actions that operators, participants and authorities, respectively, could take to promote adoption of each element.

Monitoring and measuring of progress

The CPMI would also welcome suggestions on how progress in reducing the risk of wholesale payments fraud could be monitored and measured.

Annex 1: Analysing the risk of wholesale payments fraud related to endpoint security

This Annex gives an overview of the analytical approach that the TF took to analysing the risk of wholesale payments fraud. It outlines the questions used in the preliminary stocktaking exercise.

Endpoint security relies on layered, complementary control components that collectively address the need to secure endpoints. As no single control objective can fully prevent the risk of fraud related to endpoint security, a set of multiple control objectives must be designed to work in a holistic way to strengthen the protection of endpoints, to detect and respond to potential and actual frauds in a timely manner, and to communicate to the broader payments network community in an appropriate manner to coordinate the response. In the light of the need for a holistic approach, the CPMI developed the following approach and terminology for analysing and taking stock of current arrangements in four key areas that underpin wholesale payments endpoint security:

1) Prevention of fraud

Preventive security measures are taken to reduce the likelihood of attempted or actual fraud at an endpoint. Such measures can address endpoint hardware, software, physical access,[6] logical access,[7] organisation and processes.[8] The implementation of such measures may be supported by security expectations/requirements, confirmation of adherence to security requirements, validation of adherence, use of enforcement mechanisms, providing education and training, and other tools to support prevention. Accordingly, when analysing and taking stock of current arrangements for the prevention of fraud related to endpoint security, the following questions were among those considered:

- Which parties provide tools (eg sender controls that can restrict transactions above a defined amount) to support prevention, for what and for whom?
- Which parties (eg senders, receivers, operators and their respective supervisors, regulators and overseers) have security expectations/requirements, for what and for whom?
- If a party has expectations/requirements, do they require confirmation of adherence (eg via self-assessment or assessments by third parties), how often, for what and for whom?
- If a party has expectations/requirements, do they assess/validate adherence and how often, for what and for whom?
- If a party requires confirmation and/or conducts an assessment, do they have enforcement mechanisms, for what, and for whom?

[6] The ability of people to physically gain access to a computer information system, where any such unauthorised physical access could lead to security risks and fraud. This type of access includes actual hands-on, on-site access to computer and network hardware (eg devices and data centres) or other parts of a hardware installation. Examples of safeguards are progressively restricted security zones, locked doors and intrusion alarm systems.

[7] Any type of interaction with hardware through remote access, where any such unauthorised logical access could lead to security risks and fraud. This type of access generally features software-based tools, protocols and procedures used for identification, authentication, authorisation and accountability in computer information systems. Examples of safeguards are identity and access management, intrusion detection systems, firewalls, logging and malware protection.

[8] Processes, procedures, tools, personnel and functions invoked and/or deployed across the organisation to prevent / detect / respond to any security risks and fraud. These govern, for example, activity sequences (eg the practice of requesting an approval after a payment initiation), operators (eg segregation of duties and recurrent staff vetting policies), equipment (eg bring your own device and USB policies) and/or time (eg transactions need to occur during working hours).

- Which parties provide education and training, for what and for whom?

2) Detection of fraud

Detective security measures are taken to increase the likelihood and speed of detecting actual, attempted or potential fraud at an endpoint. The implementation of such measures may be supported by security expectations/requirements, confirmation of adherence to security requirements, validation of adherence, use of enforcement mechanisms, providing education and training, and other tools to support detection. Accordingly, when analysing and taking stock of current arrangements for the detection of fraud related to endpoint security, the following questions were among those considered:

- Which parties have expectations/requirements for detection, for what and for whom?
- Which parties provide education and training, for what and for whom?
- Which parties provide tools to support detection, for what and for whom?
- If a party has expectations/requirements, do they require confirmation of adherence (eg via self-assessment or assessments by third parties), how often, for what and for whom?
- If a party has expectations/requirements, do they assess/validate adherence and how often, for what, and for whom?
- If a party requires confirmation and/or conducts an assessment, do they have enforcement mechanisms, for what and for whom?

3) Immediate response if senders, receivers or operators detect fraud

Response measures will include procedures and practices to inform relevant parties of suspected or actual fraud originating from endpoints, and to determine whether or not a payment suspected to be fraudulent is actually fraudulent. Measures may also include regular testing of capabilities and remediation of deficiencies identified through testing. Accordingly, when analysing and taking stock of current arrangements for responding to a suspected or actual fraud related to endpoint security, the following questions were among those considered:

- Which parties have expectations and requirements for senders to inform receivers, operators or law enforcement of fraudulent messages that originate at the sender's endpoint?
- Which parties require senders to investigate the origin of a fraud in the event fraudulent messages are detected at the sender's endpoint?
- Which parties have expectations and requirements for receivers to inform senders, operators or law enforcement of fraudulent messages that originate at the sender's endpoint?
- Which parties require receivers to investigate the origin of a fraud in the event fraudulent messages are detected by the receiver?
- Which parties have expectations and requirements for operators to inform senders, receivers or law enforcement of fraudulent messages that originate at the sender's endpoint?
- Which parties require the operators to investigate the origin of a fraud in the event fraudulent messages are detected by the operators?

4) Alerting the broader payments network community of attempted or actual fraud

Appropriately alerting the broader payments network community of attempted or actual fraud related to endpoint security will rely on threat intelligence functions[9] and up-to-date records of contacts, documented procedures implemented to ensure timely communication, and processes developed and implemented to alert the broader network. Accordingly, when analysing and taking stock of current arrangements for alerting the broader community of attempted or actual fraud related to endpoint security, the following questions were among those considered:

- Which parties have expectations or requirements for senders to inform the broader payments network community of attempted or actual fraudulent payment instructions/messages that may originate at the sender's endpoint?
- Which parties have expectations or requirements for receivers to inform the broader payments network community of attempted or actual fraudulent payment instructions/messages that may originate at a sender's endpoint?
- Which parties have expectations or requirements for operators to inform the broader payments network community of attempted or actual fraudulent payment instructions/messages that may originate at a sender's endpoint?
- Have any parties developed threat intelligence functions or do they use industry threat intelligence providers to gather and disseminate information about threats and threat actors?

[9] Processes, procedures, arrangements or (a group of) personnel for gathering and/or disseminating information that provides relevant and sufficient understanding for mitigating the impact of a potentially harmful event.

Annex 2: Members of the task force

Co-chairs	
National Bank of Belgium	Johan Pissens
Federal Reserve Bank of New York	Lawrence Sweet
Members	
Reserve Bank of Australia	Alison Clark
European Central Bank	Pierre Petit
Deutsche Bundesbank	Christoph Heid
Bank of Italy	Fabio Zuffranieri
Bank of Japan	Hiromi Yamaoka
Bank of Korea	Kangbong Chang
Netherlands Bank	Raymond Kleijmeer
Monetary Authority of Singapore	Nelson Chua
Swiss National Bank	Maurizio Denaro
Bank of England	David Bailey
Board of Governors of the Federal Reserve System	Jennifer Lucier
	Stuart Sperry
Secretariat	Takeshi Shirakami
	Rebecca Chmielewski

Significant contributions were also made by Nikolai Boeckx, Filip Caron and Thomas Provoost (National Bank of Belgium); Chrissanthos Tsiliberdis and Emran Islam (European Central Bank); Takashi Hamano (Bank of Japan); Justin Jacobs (Bank of England); Jeff Marquardt and Tim Maas (Board of Governors of the Federal Reserve System) and Alan Basmajian (Federal Reserve Bank of New York).