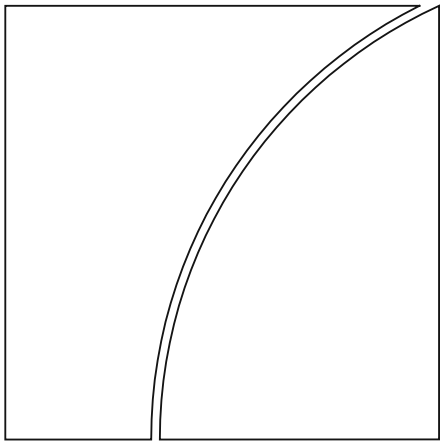
Committee on Payments and Market Infrastructures



Reducing the risk of wholesale payments fraud related to endpoint security

May 2018

BANK FOR INTERNATIONAL SETTLEMENTS

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

ISBN 978-92-9259-165-6 (print)

ISBN 978-92-9259-164-9 (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 developed a strategy to reduce the risk of wholesale payments fraud related to endpoint security (hereafter "wholesale payments fraud"), which the CPMI published for public consultation in September 2017. The final strategy reflects feedback received during that consultation.

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. To that end, each CPMI member central bank, and the CPMI as a whole, is committed to acting as a catalyst for effective and coherent operationalisation of the strategy within and across jurisdictions and systems and will monitor progress throughout 2018 and 2019 to determine the need for further action.

This report first discusses the wholesale payment ecosystem and endpoints, and the risk of wholesale payments fraud, stressing the need for a holistic approach and coordination (Section 1). It then presents the strategy, which comprises seven elements (Section 2). It then discusses the CPMI's plan to promote, support and monitor local and global progress in operationalising the strategy (Section 3), with due recognition of the need for flexibility to reflect the uniqueness of each system and jurisdiction, including the legal, regulatory, operational and technological structures and constraints under which they may operate.

1.1 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

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

the system.[2] Endpoint security is built upon measures taken with respect to endpoint hardware,[3] software, physical access,[4] logical access,[5] organisation and processes.[6]

1.2 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 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 at 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 also 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 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. In extremis, these actions could ultimately impede economic activity and disrupt 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 wholesale 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 also undertake complementary efforts. Lastly, each participant of payment systems and messaging networks has inherent

[2] It is important to note that the term "endpoint" in this document does not relate solely to parties at either end of a payment transaction chain, but rather participants of wholesale payment systems or messaging networks that can transmit and receive payment instructions on behalf of themselves or others.

[3] Endpoint hardware may include mobile devices, laptop or desktop PCs, and other equipment such as servers and network devices. Endpoint hardware may or may not be controlled directly by the operator of a wholesale payment system or messaging network.

[4] Physical access refers to 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.

[5] Logical access refers to 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, and logging and malware protection.

[6] Processes, procedures, tools, personnel and functions invoked and/or deployed across the organisation to prevent, detect and 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).

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 all relevant parties, resulting in an insufficient level of action and investment – individually and collectively – 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 wholesale payment systems and messaging networks, their participants and relevant authorities, take a holistic and more coordinated approach to guarding against the potential loss of confidence in the integrity of the wholesale payment ecosystem as a whole.

2. 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 wholesale payment systems and messaging networks, their participants and the respective regulators, supervisors and overseers of these operators and participants.[7] 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 wholesale 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. In addition, based on input received during the public consultation, Annex 1 provides a number of points that could be taken into consideration by operators, participants and other relevant stakeholders as they move forward in developing or implementing their plans for operationalising the strategy.

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 the 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 wholesale 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 wholesale payment system or a messaging network, their respective participants and the respective regulators, supervisors and overseers of these operators and participants.

Element 1: Identify and understand the range of risks

The operator and participants of a wholesale 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.

Element 2: Establish endpoint security requirements

The operator of a wholesale payment system or a messaging network should have 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 wholesale payments network community to evolving fraud threats. In addition to the requirements established by the operator of a wholesale payment system or a messaging

[7] The terms "operator(s)" and "participant(s)" throughout this document 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).

network, each participant of the payment system or messaging network should identify and establish its own, supplemental risk-based endpoint security arrangements as needed.

Element 3: Promote adherence

Based upon the understanding of the risks and the endpoint security requirements of a wholesale payment system or a messaging network, the operator and participants of the payment system or messaging network should have processes as necessary to help promote adherence to their respective endpoint security requirements.

Element 4: Provide and use information and tools to improve prevention and detection

The operator and participants of a wholesale 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 attempted wholesale payments fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible.

Element 5: Respond in a timely way to potential fraud

The operator and participants of a wholesale payment system or a messaging network should have 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 and communication of, and response to, a request to take action concerning a potentially fraudulent payment instruction when detected. Such procedures and practices should not alter or affect the finality of any payment that has already been settled.

Element 6: Support ongoing education, awareness and information-sharing

The operator and participants of a wholesale 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 and feasible, information-sharing about evolving endpoint security risks and risk controls.

Element 7: Learn, evolve and coordinate

The operator and participants of a wholesale 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 wholesale payment systems and messaging networks should seek to coordinate approaches for strengthening endpoint security across systems and networks in order to achieve potential efficiencies where possible and appropriate. Similarly, regulators, supervisors and overseers of wholesale payment systems and messaging networks and participants of wholesale payment systems and messaging networks should review and update their regulatory/supervisory/oversight expectations and assessment programmes as appropriate to reflect the evolving risk mitigation strategies.

3. Promoting, supporting and monitoring progress in operationalising the strategy

The CPMI recognises that successful operationalisation of the strategy depends on operators, participants and other relevant private sector and public sector stakeholders in each jurisdiction engaging actively in and taking ownership of developing and carrying out an appropriate action plan for their respective jurisdictions.

Accordingly, effective operationalisation of the strategy can be supported by the following actions.

1) Obtaining the commitment of all relevant stakeholders in each system and jurisdiction to operationalise the strategy and to engage and coordinate in identifying and taking appropriate action.

2) Supporting the necessary flexibility[8] that allows stakeholders to reflect the uniqueness of each system and jurisdiction in determining how best to operationalise the strategy, with the clear understanding that flexibility should be exercised for the purpose of achieving the most effective outcomes and should not lead to inaction or slow progress.

3) Providing opportunities for payment systems/messaging networks to coordinate and, if relevant and appropriate, to harmonise the actions they may take when operationalising the strategy, both within and across jurisdictions, so as to maximise potential efficiencies and to avoid potential inconsistencies in requirements, processes and practices across systems and jurisdictions.

4) Establishing a clear allocation of tasks, responsibilities and timetable for operationalising the strategy and for monitoring progress.

At the same time, each CPMI member central bank, and the CPMI as a whole, is committed to acting as a catalyst for success by taking supportive steps to promote effective and coherent operationalisation of the strategy within and across jurisdictions and systems. To that end, each CPMI member central bank, and the CPMI as a whole, will monitor progress throughout 2018 and 2019 to determine the need for further action. In particular, the CPMI and its members intend to undertake the following steps to advance the operationalisation of the strategy:

1) *The CPMI* will act as a driving force to promote timely progress in the operationalisation of the strategy by:

    a. monitoring local progress via updates from individual CPMI members;

    b. supporting cross-system coordination and, if and as relevant, appropriate harmonisation (eg via CPMI sponsorship of industry workshops), to address common issues or enhancement opportunities as identified via monitoring of local progress; and

    c. providing outreach to a wide range of non-CPMI central banks/jurisdictions to promote global awareness, support and operationalisation of the strategy.

2) *Each CPMI member central bank* will use its available roles (eg as catalyst, operator, overseer), as relevant and appropriate, to advance operationalisation of the strategy within the central bank's jurisdiction. In particular, each CPMI member central bank intends to promote and support local progress in its jurisdiction by:

[8] Such flexibility relates to the *substance* of security requirements, process and procedures, and other arrangements that a wholesale payment system or messaging network establishes as well as the *modality* whereby relevant stakeholders engage and coordinate, reflecting eg market structure or regulatory/supervisory arrangements in a jurisdiction.

a. promoting appropriate and timely progress in its local jurisdiction and monitoring progress;

b. promoting engagement and cooperation among relevant stakeholders in operationalising the strategy, as necessary and appropriate;

c. encouraging the establishment of responsibilities and timelines for action that are clear and consistent with successful overall operationalisation of the strategy;

d. identifying significant obstacles to operationalisation or enhancement opportunities that might benefit from cross-system coordination or harmonisation; and

e. providing the CPMI with periodic updates on local progress.

Annex 1: Points for consideration for operationalising the strategy

Comments submitted during the consultation period indicate that many operators, participants and other stakeholders are already deeply engaged in developing or implementing plans to reduce the risk of wholesale payments fraud related to endpoint security. Based on their experiences to date, commenters submitted a number of potentially relevant points that could be taken into consideration by other operators, participants and relevant stakeholders as they, in turn, move forward in developing or implementing their own plans for operationalising the strategy. Below is a summary of the main points for consideration offered by commenters during the consultation period.

Element 1 – Identify and understand the range of risks

The range of risks may differ across systems and jurisdictions, given: the uniqueness of different wholesale payment systems and messaging networks and their participants; the legal, regulatory and supervisory regimes that they are subject to; and differences among their respective stakeholders. It is therefore important to clearly identify the distinct roles and responsibilities for all stakeholders in the wholesale payment ecosystem, and for each to consider its specific range of risks. For example, participants can serve multiple roles, such as originator, originator's bank, payment service provider for other parties, beneficiary, beneficiary's bank or intermediary bank in the payment chain, and the associated risks will differ depending on their specific roles.

The boundaries of endpoint security risk may go beyond payment systems and their direct participants. Operators will need to be mindful of risks borne from indirect participants and others involved in the correspondent banking system.

Element 2 – Establish endpoint security requirements

Endpoint security requirements may relate to participants' hardware, software, physical access to relevant systems and interfaces, logical access, organisation and processes. Requirements could be principles-based, specifying security objectives that can be met by a variety of technologies and controls, or could contain more specific measures, as appropriate to the design of a wholesale payment system or messaging network.

Operators of payment systems and messaging networks could leverage existing broadly supported security frameworks, where those frameworks are assessed to be comprehensive and effective. Those frameworks could be supplemented with context-specific requirements if required. Stakeholders within a jurisdiction may collaborate to avoid potentially duplicative or conflicting requirements across different payment systems and messaging networks.

Operators of payment systems and messaging networks will need flexibility to determine endpoint security requirements that are tailored to their legal, regulatory and supervisory regimes and are practical and effective given the unique attributes of their systems and their participants.

When endpoint requirements are established, care should be taken to help ensure that they do not unduly shift legal liability away from participants that ought to remain responsible for securing their own endpoint.

Element 3 – Promote adherence

There is a range of potential options for promoting adherence to endpoint security requirements which include but are not limited to self-certification, internal audit, supervisory review, external audit, external certification or a combination thereof. Operators of wholesale payment systems and messaging networks will need to consider a range of options and decide on establishing an effective programme to promote adherence based on the design of their own system and the legal, regulatory and supervisory regimes that they are subject to.

Operators will also need to consider the consequences if a participant's endpoint security is determined to be deficient. They may consider establishing rules, procedures and processes to address endpoint security weaknesses, including (i) requesting remediation plans; (ii) providing to or agreeing with the participant an appropriate time frame for remediation, with the potential of limiting access in the event of no remediation; (iii) providing passive transparency on the security posture to peers; and (iv) actively reporting to relevant stakeholders such as supervisory authorities that play a role in promoting and/or assuring adherence to endpoint security requirements. Operators should exercise care when considering the possibility of restricting or suspending such participants' access to their systems or networks.

In all cases, operators should consider how to ensure that information related to the security measures and posture of participants is appropriately protected and kept confidential.

Element 4 – Provide and use information and tools to improve prevention and detection

The provision and use of tools to prevent and detect fraud could help improve endpoint security. The types of tools that can be made available will depend on the design of a wholesale payment system or messaging network.

Operators of payment systems or messaging networks could work together with their participants, and other stakeholders, to evaluate what types of information and tools could effectively support the prevention and detection of wholesale payment fraud at the endpoints. These might include (i) participant-defined payment limits (eg payments will be processed only when they are addressed to a known correspondent within business hours and amount limits); (ii) payment screening against self-determined parameters; (iii) detection of unusual or uncharacteristic payment patterns (eg in terms of timing, value, volume or location); and (iv) frequent and timely (intraday) reconciliations.

Careful consideration should be given to helping ensure that ultimate responsibility and legal liability for fraudulent payments will not be unduly shifted from participants that ought to remain responsible for securing their own endpoint. For example, participants remain responsible for employing and parameterising these tools as well as dealing with any alerts generated.

Element 5 – Respond in a timely way to potential fraud

Operators of wholesale payment systems and messaging networks should assess what arrangements are in place in their jurisdiction for the response to fraud, and consider what role they should take in facilitating participants' requests for cancellation of payment instructions or requests for return of funds. These arrangements will be affected by the design of their own systems. For example, the operator may not be directly involved, and responses may be through bilateral communication between participants.

Operators, in consultation with their participants, should consider whether these communications protocols should include the relevant regulators, supervisors and overseers, and other law enforcement authorities.

At the same time, it is important that response to fraud or possible fraudulent transactions should not compromise the irrevocability and alter or affect the finality of any payment that has already been settled.

There are legal constraints related to privacy/data protection and information-sharing. Stakeholders will need to consider how to best share information, taking into consideration the constraints applicable in their jurisdiction. Further, due consideration should be given to potential liability if participants or others provide information which is later found to be erroneous, inaccurate or incomplete.

Element 6 – Support ongoing education, awareness and information-sharing

Operators of wholesale payment system and messaging networks could establish processes for ongoing education, awareness and information-sharing about security risks and good security practices.

There are legal constraints related to privacy/data protection and information-sharing. Stakeholders will need to consider how to best share information, taking into consideration the constraints applicable in their jurisdiction, especially where the information to be shared is sensitive and not entirely generic. Further, due consideration should be given to potential liability if participants or others provide information which is later found to be erroneous, inaccurate or incomplete.

National bodies and industry groups or other information exchange mechanisms (eg information-sharing and analysis centres (ISACs)) could be leveraged to help share information and create awareness in the industry.

Element 7 – Learn, evolve and coordinate

Operators of wholesale payment systems and messaging networks will need to update their endpoint security requirements as the threat landscape evolves. Operators could use the results of their adherence programmes to conduct thematic analysis of weaknesses in security across their participants or network, and consider enhancing their endpoint security requirements.

Industry stakeholders could monitor emerging technologies and evolving security arrangements with a view to developing best practices and assisting all stakeholders in learning about and adapting to the evolving threat environment.

There could be benefits to coordinating, and potentially harmonising, across jurisdictions actions taken to operationalise the strategy. For instance, coordinating approaches could help avoid inconsistency and unnecessary duplication of efforts or requirements that could potentially cut across borders and affect participants of payment systems in multiple jurisdictions.

Annex 2: 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,[9] logical access,[10] organisation and processes.[11] 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, does it require confirmation of adherence (eg via self-assessment or assessments by third parties)? If so, how often, for what and for whom?
- If a party has expectations/requirements, does it assess/validate adherence? If so, how often, for what and for whom?
- If a party requires confirmation and/or conducts an assessment, does it have enforcement mechanisms? If so, for what and for whom?
- 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.

[9] See footnote 4 above.

[10] See footnote 5 above.

[11] See footnote 6 above.

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, does it require confirmation of adherence (eg via self-assessment or assessments by third parties)? If so, how often, for what and for whom?
- If a party has expectations/requirements, does it assess/validate adherence? If so, how often, for what and for whom?
- If a party requires confirmation and/or conducts an assessment, does it have enforcement mechanisms? If so, 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 that 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 that 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 that 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[12] 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:

[12] 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.

- 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?

Annex 3: 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
Bank of Canada	Chris Loken
European Central Bank	Pierre Petit
Bank of France	Clay Youale
Deutsche Bundesbank	Christoph Heid
Bank of Italy	Fabio Zuffranieri
Bank of Japan	Hiromi Yamaoka
Bank of Korea	Kangbong Chang (until August 2017)
	Teukrok Kang (since August 2017)
Netherlands Bank	Raymond Kleijmeer
Central Bank of the Russian Federation	Savva Morozov
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
	Luca Colantoni

Significant contributions were also made by Nikolai Boeckx, Filip Caron and Thomas Provoost (National Bank of Belgium); Emran Islam and Chrissanthos Tsiliberdis (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); Rebecca Chmielewski (Federal Reserve Bank of Chicago); and Alan Basmajian (Federal Reserve Bank of New York).