Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Version 1

October 2019

Reducing the risk of wholesale payments fraud related to endpoint security: a toolkit

Introduction

The Committee on Payments and Market Infrastructures (CPMI) has prepared this "toolkit" to support central banks that wish to reduce the risk of wholesale payments fraud related to endpoint security in their institutions and jurisdictions. To reduce this risk, the CPMI has developed a strategy with seven elements designed to address all areas relevant to preventing, detecting, responding to and communicating about wholesale payment fraud.

This toolkit provides context for the CPMI strategy and identifies steps that central banks could take to operationalise the strategy in a chronological sequence: (i) promotion; (ii) initial stocktaking; (iii) engagement with stakeholders; (iv) development of an action plan; and (v) monitoring progress. Key documents used by the CPMI and its members in their own operationalisation are included at each stage. Central banks may choose to operationalise individually, as part of a regional effort, or both.

This is a "living document". As central banks, operators, participants and other stakeholders progress, and as their experiences and emerging practices for achieving the intended outcomes of the strategy develop further, the toolkit will also evolve. In addition, not all emerging practices will be appropriate for all jurisdictions, and there is no "one size fits all" approach to operationalising the strategy. Instead, this toolkit aids central banks in understanding which emerging practices are relevant and appropriate, and forming their own judgment.

Other resources

Online tutorials covering the strategy are available. The Financial Stability Institute (FSI) at the Bank for International Settlements (BIS) has agreed to make tutorials covering wholesale payments security and the CPMI-IOSCO cyber resilience guidance freely available to central banks upon request. Central banks interested in these materials should contact the FSI Connect customer support team at fsiconnect@bis.org.

CPMI members and its secretariat frequently attend regional events to explain and update central banks about current work. Central banks interested in learning about relevant events in their region can contact the CPMI secretariat for more details at cpmi@bis.org.

Operationalising the strategy

Key document

1. CPMI report *Reducing the risk of wholesale payments fraud related to endpoint security*

The CPMI strategy is set out in the 2018 report *Reducing the risk of wholesale payments fraud related to endpoint security* (key document 1). Operationalisation of the strategy depends on central banks, operators, participants and other stakeholders engaging and taking ownership for developing and carrying out an action plan for their institutions and jurisdictions.

Promoting the strategy

Key document

2. GEM and CPMI chairs' invitation letter to non-GEM central bank Governors

A first step central banks may wish to consider, either individually or as a part of a regional effort, is to adopt and to announce their commitment to promoting, supporting and monitoring progress in operationalising the strategy in their respective institutions and jurisdictions.

The chairs of the BIS Global Economy Meeting (GEM) and the CPMI wrote to all non-GEM and non-CPMI central banks in December 2018, encouraging them to consider the strategy and inviting them to join in the effort to reduce the risk of wholesale payments fraud related to endpoint security (key document 2). In the press release announcing their approval of the report, the GEM Governors announced their support and commitment to putting the strategy into practice within each of their institutions and jurisdictions. The CPMI report itself also states that "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".

Taking stock of current arrangements

Key document

3. Stocktaking questions to aid an initial consideration of current arrangements

Following a commitment to operationalise the strategy, a central bank may wish to take stock of the current arrangements in the main areas that underpin wholesale payments endpoint security. A number of questions could be considered in such a stocktaking exercise, which could follow the intended outcomes of the strategy and emerging practices to meet those outcomes (key document 3). Central banks could use this initial stocktaking of current arrangements to help them identify existing gaps and weaknesses and determine the need for further action.

Engaging with relevant stakeholders

Key document

4. Slide pack explaining the CPMI strategy

Once current arrangements are understood and the need for further action identified, central banks can engage relevant operators, participants and other stakeholders to promote their awareness of the strategy and enlist their commitment to support its operationalisation (key document 4). These operators, participants and other stakeholders may be inside or outside the central bank. One way the CPMI has engaged with relevant stakeholders to promote awareness and to facilitate industry-wide operationalisation of the strategy is through industry workshops.

Developing an action plan to operationalise the strategy

Key document

5. Intended outcomes and example emerging practices to operationalise the strategy

Once relevant stakeholders are identified, they can be encouraged to develop plans to achieve the intended outcomes of the strategy. A central bank can consider assigning a project team within the central

bank with responsibility for developing an overall plan, or coordinating the development of such a plan by relevant operators, participants and other stakeholders, to achieve the intended outcomes of the strategy.

Understanding how best to achieve each of the intended outcomes of the strategy is not always simple, since there is no "one size fits all" approach that is suitable for all systems and jurisdictions. As part of its engagement with operators and participants of wholesale payment systems and messaging networks in all CPMI member jurisdictions, the CPMI has collected and compiled a number of examples of emerging practices for achieving the intended outcomes of each of the strategy's elements as well as potentially relevant points that could be taken into consideration in developing or implementing plans (key document 5). The emerging practices are not exhaustive, or necessarily appropriate for every jurisdiction, but act as a guide and aide for understanding the intended outcomes and elements.

Monitoring progress

Key document

6. Template to monitor progress in operationalising the strategy

A central bank can also consider assigning a project team to monitor progress with respect to each wholesale payments system and messaging network in its jurisdiction, including those that might be operated by the central bank itself. Such monitoring can support the central bank's ability to identify any obstacles and challenges and determine the need for further action. A standard template is provided that central banks could use to monitor progress (key document 6).

Key documents

1. CPMI report *Reducing the risk of wholesale payments fraud related to endpoint security*
2. GEM and CPMI chairs' invitation letter to non-GEM central bank Governors
3. Stocktaking questions to aid an initial consideration of current arrangements
4. Slide pack explaining the CPMI strategy
5. Intended outcomes and example emerging practices to operationalise the strategy
6. Template to monitor progress in operationalising the strategy

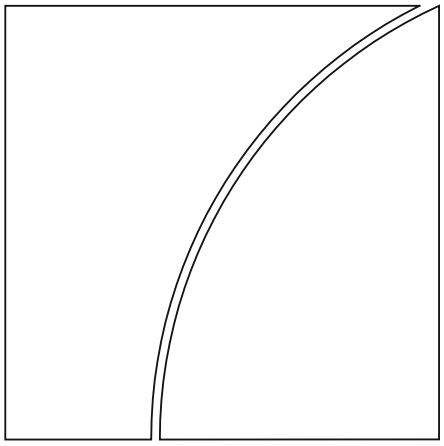
Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Key document 1

CPMI report, Reducing the risk of wholesale payments fraud related to endpoint security

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 1

2. Strategy for reducing the risk of wholesale payments fraud related to endpoint security 4

3. Promoting, supporting and monitoring progress in operationalisation of the strategy 6

Annex 1: Points for consideration for operationalising the strategy 8

Annex 2: Analysing the risk of wholesale payments fraud related to endpoint security 11

Annex 3: Members of the task force 14

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).

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Key document 2

GEM and CPMI chairs invitation letter to non-GEM central bank governors

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Restricted

To: Central bank Governors

5 December 2018

Strategy to improve wholesale payments security

Recent incidents have demonstrated that the security of the payments ecosystem is under threat. We would like to bring to your attention a high-level strategy that the central bank Governors of the BIS Global Economy Meeting (GEM) have endorsed and are promoting globally in order to improve wholesale payments security. We hope that you might also lend your support to this key initiative.

A key cause for concern is that systems are particularly vulnerable to fraud at crossover points, such as between a payment system and a messaging network, between a messaging network and a network participant, or between a payment system and a participant. Weaknesses at these so-called endpoints have been exploited to commit fraud and the fraudsters are becoming increasingly sophisticated. This could disrupt the functioning of the global financial system and, potentially, undermine public confidence in its integrity.

In this light, the Committee on Payments and Market Infrastructures (CPMI) developed a comprehensive strategy to reduce the risk of payments fraud related to endpoint security. The strategy was set out in a report published by the CPMI in May 2018, *Reducing the risk of wholesale payments fraud related to endpoint security*. The strategy consists of seven elements designed to address all areas relevant to preventing, detecting, responding to and communicating about wholesale payments fraud.

The strategy's success depends crucially on active engagement and coordinated action by the operators and participants of wholesale payments systems and messaging networks as well as other relevant private and public sector stakeholders. As central banks themselves are operators, users and/or overseers of payment systems and messaging networks, we are uniquely positioned to take a leading role in promoting and supporting the progress of the strategy. Accordingly, when the GEM Governors endorsed the strategy, they also expressed their commitment to putting it into practice within their institutions and jurisdictions.

In addition, each CPMI member central bank, and the CPMI as a whole, are 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.

Against this background, we would like to invite you to join us in these efforts, and to consider how relevant this risk is to your institution and jurisdiction and how appropriate the CPMI strategy is for your circumstances.

The CPMI has started liaising with regional groups of central banks across the world and the BIS Financial Stability Institute (FSI) with a view to presenting the strategy to all relevant stakeholders. This two-way dialogue is a key part of the CPMI's aspiration for widespread adoption of the endpoint security strategy. We hope that you will be able to participate in relevant seminars and workshops on the CPMI strategy organised by the regional groups in cooperation with us.

In this conjunction, the CPMI has developed study material on the CPMI strategy together with the FSI. This material was released on 29 November and is available as part of the FSI connect tutorials, a web-based learning portal for subscribed institutions.

We look forward to working together with you in this important initiative to reinforce confidence in the integrity of the wholesale payments ecosystem. Please contact the Secretariat (morten.bech@bis.org) if you have any questions.

Yours sincerely

Mark Carney — GEM Chair

Benoît Cœuré — CPMI Chair

cc: Governors of the BIS Global Economy Meeting

Mr Fernando Restoy, Chair of the BIS Financial Stability Institute

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Key document 3

Stocktaking questions to aid an initial consideration of current arrangements

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Stocktaking questions to aid an initial consideration of current arrangements

Introduction

Following a commitment to operationalise the strategy, a central bank may wish to take stock of the current arrangements in the main areas that underpin wholesale payments endpoint security.

This document sets out a number of questions that could be considered in such a stock-taking exercise, and follows the elements of the strategy, their intended outcomes and emerging practices to meet those outcomes. "Key questions" query if the outcomes have been met, and "further questions" query how they could have been met (taking into account identified emerging practices).

The questions are not exhaustive, other practices could exist that support the intended outcomes of the strategy, and practices identified for one system or jurisdiction may not necessarily be relevant or appropriate for another. However, central banks can use this initial stocktaking of current arrangements to help them identify potential gaps, weaknesses and enhancement opportunities, as well as determining the need for further action.

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."

Key questions

- Does the operator consider the range of risks that the individual endpoints of its system pose to the collective confidence in the integrity of the system/network?
- Do participants have an awareness of the range of risks that individual endpoints of the system pose to their collective confidence in the integrity of the system/network?

Further questions

- Does the operator conduct formal, annual assessments to identify endpoint security risks? The assessment should explicitly take into consideration the risk of participants and other stakeholders losing confidence in the integrity to the overall system.
- Does the operator use external vendors to help with the identification of endpoint security risks and penetration testing?
- Does the operator engage with regional payment system bodies to identify and understand cross-cutting endpoint security risks?
- Does the operator have procedures to report internally potential fraud attempts or incidents of unauthorised transactions to inform and support its evolving risk management?
- Does the operator have an ongoing process to raise and maintain participant awareness of the importance of endpoint security through workshops, seminars and related communication channels?
- Do stakeholders in the system/network (eg, the central bank, the operator, participant/user groups) employ communication channels (eg notices, letters, meetings, speeches, educational workshops, conference presentations) to explain and emphasise the need for collective and coordinated action to address the risk of losing confidence in the integrity of the overall system/network?

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

Key questions

- Has the operator established requirements for its participants to prevent fraud?
- Has the operator established requirements for its participants to detect attempted fraud?
- Has the operator established requirements for its participants regarding their immediate response to potential fraud?
- Has the operator established requirements for its participants, when appropriate, to alert the broader payments network community to evolving fraud threats?
- Do participants conduct reviews to determine what, if any, supplemental risk-based endpoint security arrangements they may need to establish for themselves?

Further questions

- Does the operator have established requirements for participants to prevent and detect fraud with respect to each participant's endpoint hardware, software, physical access, logical access, organisation and processes?
- Does the operator encourage or require participants to use available information and/or tools to prevent fraud by identifying and blocking in "real-time" potentially fraudulent payments before they are sent (see also element 5)?
- Does the operator encourage or require participants to adopt an explicit framework to detect potential fraud (eg by receiving and checking ex post "out of band" reports of sent payments and notices of changes to participant access credentials) (see also element 4)?
- Does the operator encourage or require participants to use pre-defined procedures and practices (including contact information) for their timely initiation of, and immediate response to, a request to take action concerning a potentially fraudulent payment instruction (including during off-hours) (see also element 5)?
- Does the operator encourage or require participants to alert the broader payments community to evolving threats and risks (eg via the operator, the participants' supervisors, or the relevant ISACs) (see also element 6)?
- Do the operator's requirements (ie for preventing fraud; for detecting fraud; for the immediate response to fraud; and for alerting the broader payments network community to evolving fraud threats) feature explicitly in system/network rules?

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."

Key questions

- Are there processes to promote participants' adherence to their respective endpoint security requirements?

Further questions

- Does the operator require each participant to self-attest at least annually to the participant's adherence to the security requirements of operators?
- Does the operator require an independent institution to carry out mandatory compliance assessments on participants?
- Are participants required to conduct self-assessments of adherence to the established requirements at least annually with the help of an independent third party to provide a review?
- Has the operator established incentives for participants to adhere to requirements (eg by establishing a process for the review of self-attestations/monitoring questionnaires by counterparties, internal/external auditors, supervisors, or other relevant stakeholders)?
- Has the operator established rules, procedures and processes for participants to address identified endpoint security weaknesses, for example by (i) requiring remediation plans; (ii) providing to or agreeing with the participant an appropriate time frame for remediation, with the potential of limiting the participant's access to the system in the event of insufficient remediation; and (iii) reporting a participant's insufficient adherence to the participant's direct supervisory authority?
- Are participants obliged to adhere to requirements and put in place mechanisms to review, identify and remedy any potential gaps in adherence?
- Do the expectations and assessment programmes of the participants' supervisors reflect, as appropriate, all relevant endpoint security requirements applicable to participants (see also element 7)?

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."

Key questions

- Does the operator use information and tools to prevent fraud to the extent reasonably practicable and legally permissible and feasible?
- Does the operator use information and tools to detect fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible?
- Do participants use information and tools to prevent fraud to the extent reasonably practicable and legally permissible and feasible?
- Do participants use information and tools to detect fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible?

Further questions

- Does the operator use information and tools to prevent fraud by identifying and, with relevant participant's consent/involvement, block in "real-time" potentially fraudulent payments before they are processed. This includes (i) tools to authenticate and prevent settlement of anomalous transactions, (ii) tools to block fraudulent transactions submitted and awaiting settlement on instruction, (iii) allowing participants to set "whitelists" of other participants who can be sent funds, (iv) automated fraud intelligence sharing with participants?
- Does the operator use information and tools to detect fraud by identifying and investigating, in a timely manner, potentially fraudulent payments that may have been processed?
- Do participants use information and tools (either developed internally or provided externally by the operator or a third party) to prevent fraud by identifying and blocking in "real-time" potentially fraudulent payments before they are sent, on the basis of parameters set by participants (eg, to restrict outgoing payments above a certain amount, or to certain payees, or that are intiated outside certain hours)?
- Do participants use information and tools (eg ex-post "out of band" reports of sent payments and notices of changes to access credentials provided by the operator) to detect fraud by identifying and investigating in a timely manner potentially fraudulent payments that may have been sent?
- Does the operator provide tools to participants to identify and block outgoing payments in "real time" with the most restrictive settings predefined and selected by the operator for each participant (participants then have the ability to adjust the settings of the tools based on their own activity and judgment)?
- Do the operator and participants take a risk-based approach to using information and tools to prevent and detect potential fraud, such as by focusing on the identification and blocking in "real time"of potentially fraudulent payments sent by smaller system participants and correspondent banking clients?

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."

Key questions

- Has the operator adopted procedures and practices that support its timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection?
- Have participants, collectively and individually, adopted procedures and practices that support their timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection?

Further questions

- Does the operator have 24x7 emergency hotlines and contact lists (for itself and its participants), along with internal escalation procedures, tools and staff training programmes, to enable the operator to block pending payments that are identified by itself or its participants as potentially fraudulent?
- Do participants have 24x7 emergency hotlines, contact lists and internal escalation procedures, tools and staff training programmes, to enable each participant to initiate and to respond to requests to block pending payments that are identified by itself, the operator, or other participants as potentially fraudulent?
- Do operators and participants consider the potential need for, and where necessary develop, indemnity agreements to support their timely response to requests to take action without unduly shifting or creating legal liability?
- Do participants actively engage in industry groups to develop best practices for the timely fraud response?
- Do operators and participants employ industry-wide table top scenario exercises to identify and address potential barriers to a speedy response to fraud?

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."

Key questions

- Do the operator and participants collaborate in support of information-sharing and ongoing education and awareness about evolving endpoint security risks and risk controls?

Further questions

- Does the operator conduct outreach to participants and promote information-sharing efforts that connect different industry groups (eg banks and credit unions)?
- Do the operator and participants leverage existing cyber security working groups to incorporate fraud-related elements of the strategy into their plans?
- Do the operator and participants leverage existing national bodies and industry groups and other information exchange mechanisms (eg information-sharing and analysis centres (ISACs)) to share information and to create awareness of evolving risks and risk controls?
- Do participants leverage existing industry information sharing organisations to voluntarily alert the broader payments network community to evolving fraud threats?
- Do the operator and participants jointly determine how best to share information given the relevant legal constraints related to privacy/data protection and other sensitivities?
- Does the operator provide informative reports, training sessions, roundtables and other forms of education about the evolving risks and risk controls to participants through various means?

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 obtain potential efficiencies where possible and appropriate. Similarly, regulators, supervisors and overseers of wholesale payment systems and messaging network 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."

Key questions

- Does the operator monitor evolving endpoint security risks and risk controls?
- Do participants, collectively or individually, monitoring evolving endpoint security risks and risk controls?
- Does the operator and, to the extent practicable, do participants, coordinate approaches for strengthening endpoint security with other relevant systems and networks where possible and appropriate?
- Do the expectations and assessment programmes of regulators, supervisors and overseers of the operator reflect, as appropriate, the relevant intended outcomes of this strategy?
- Do the expectations and assessment programmes of the regulators, supervisors and overseers of the participants reflect, as appropriate, the relevant intended outcomes of this strategy?

Further questions

- Does the operator regularly interact with threat intelligence organisations, both commercial and governmental, to report and to receive updates regarding endpoint security incidents?
- Do participants interact, to the extent practicable, with threat intelligence organisations, both commercial and governmental, to report and to receive updates regarding endpoint security incidents?
- Does the operator regularly engage with participants to report and to receive updates regarding endpoint security incidents?
- Does the operator engage and exchange information with other operators on evolving endpoint security approaches, both bilaterally and through multilateral operator groups?
- Do participants engage and exchange information on their respective evolving endpoint security approaches through various domestic and international industry groups?
- Did the central bank inform the operator's relevant authority (ie regulator/supervisor/overseer) of the strategy and its intended outcomes, to support the authority's review and updating of its endpoint security expectations and assessment program, as appropriate?
- Did the central bank inform the participants' relevant authorities (ie regulators/supervisors/ overseers) of the strategy and its intended outcomes, to support the authorities' review and updating of their endpoint security expectations and assessment programs, as appropriate?

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Key document 4

Slide pack explaining the CPMI strategy

Committee on Payments and Market Infrastructures

BIS

Reducing the risk of wholesale payments fraud related to endpoint security

Outline

- Background to CPMI report & strategy of May 2018
- What do we mean by “endpoint security”?
- Why is wholesale payments fraud so challenging?
- Overview of the CPMI strategy
- Overview of progress
- Next steps in operationalising the strategy

Annex: The seven elements and intended outcomes of the CPMI strategy

Background to CPMI report & strategy of May 2018

- Establishment of the CPMI Wholesale Payments Security Task Force announced in September 2016
  - To explore and address the broader, systemic vulnerabilities related to endpoint security, as revealed by the Bangladesh Bank event and other high profile cases
    - Bangladesh Bank was a participant, or "endpoint", of the SWIFT payment messaging network
- Motivated by central bank concerns for financial system stability and in our roles as operators, overseers, supervisors and participants in the wholesale payments ecosystem

What do we mean by “endpoint security”?

- Endpoint: a point in place and time at which payment instruction information is exchanged between two parties in the ecosystem, such as between:
  - a messaging network and a participant in the network
  - a payment system and a participant in the system
  - a payment system and a messaging network
  - one participant and another participant
- Endpoint does not relate solely to parties at either end of a payment transaction chain, but rather to each link in the chain as it transmits or receives payment instructions on behalf of themselves or others
- Endpoint security is built upon measures taken with respect to endpoint hardware, software, physical access, and logical access, along with the organisation and processes that surround them
  - Involves not only prevention, but also detection, response, and the need to continually learn and evolve

Why is wholesale payments fraud so challenging?

- Wholesale payments fraud is sophisticated and evolving
  - Reflects both criminal and state-sponsored actors that can be well-funded and quite determined
- To be sure, each participant -- or "endpoint" -- in a payment system or payment messaging network has a strong incentive to prevent fraud
  - Individual financial loss and reputational risk
- In the wake of notable fraud events, it became apparent that interconnectedness also creates major externalities in the form of potential system-wide risk
  - Individual breaches can undermine confidence in the integrity of the system
  - Defensive responses can lead to gridlock and reduced market liquidity
  - A large and sudden build up of unsettled payments could trigger broader financial system instability and impede economic activity
- Operators cannot solve this alone; nor can individual participants
- Requires a ***holistic strategy and coordinated action*** by all stakeholders
  - To "internalise" these system-wide "externalities"
  - To develop solutions that are effective…and also cost effective

Overview of the CPMI strategy: seven elements

1. **Identify and understand the range of risks**
   - To ensure operators and participants understand their individual risks and their collective risk of loss in confidence in the integrity of the wholesale payment system
2. **Establish endpoint security requirements**
   - To identify and address any gaps for prevention, detection, and response
3. **Promote adherence**
   - To provide incentives and confidence that endpoint requirements are being met
4. **Provide and use info and tools to improve prevention and detection**
   - To enhance current capabilities of operators and participants
5. **Respond in a timely way to potential fraud**
   - To ensure participants and operators know who to contact and how each should respond
6. **Support ongoing education, awareness, and information sharing**
   - To promote operator and participant collaboration on procedures, processes, and resources
7. **Learn, evolve, and coordinate**
   - To monitor and to keep up with ever-changing risks

Next steps in operationalising the strategy

- The Governors of the Global Economy Meeting have each committed to putting the strategy into practice within their institutions and jurisdiction
  - This requires operators, participants, and other relevant stakeholders in each system/jurisdiction to take ownership for developing and carrying out their parts in an appropriate, overall action plan
- Each individual CPMI member has committed to support the strategy by:
  - Promoting and monitoring progress in its respective jurisdiction
  - Leveraging its roles as catalyst, operator, overseer, and/or supervisor
    - Many members have teams specifically tasked with promoting and monitoring progress in the wholesale payments ecosystem
- The CPMI, as a committee, has committed to support the strategy by:
  - Promoting and monitoring timely progress among its members
  - Supporting cross-system and cross-country coordination
  - Promoting awareness and supporting adoption by all central banks around the world
- Global industry workshop held in February
  - Significant progress and momentum across CPMI member jurisdictions
  - Emerging set of practices for operationalising the strategy drafted and shared
  - Follow up workshop is planned for December 2019

Annex:

The seven elements and intended outcomes of the CPMI strategy

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."

- **Intended outcomes**:
  - The operator takes into consideration the range of risks that the individual endpoints of its system pose to the collective confidence in the integrity of the system/network itself (1.1)
  - Participants are aware of the range of risks that individual endpoints of the system pose to their collective confidence in the integrity of the system/network itself (1.2)

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

- **Intended outcomes**:
  - The operator has established requirements for its participants to prevent fraud (2.1)
  - The operator has established requirements for its participants to detect attempted fraud (2.2)
  - The operator has established requirements for its participants regarding their immediate response to potential fraud (2.3)
  - The operator has established requirements for its participants, when appropriate, to alert the broader payments network community to evolving fraud threats (2.4)
  - Participants conduct reviews to determine what, if any, supplemental risk-based endpoint security arrangements they may need to establish for themselves (2.5)

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."

- **Intended outcome**:
  - Processes exist to promote participants' adherence to their respective endpoint security requirements (3.1)

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."

- **Intended outcomes**:
  - The operator has and uses information and tools to *prevent* fraud to the extent reasonably practicable and legally permissible and feasible (4.1)
  - The operator has and uses information and tools to *detect* fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible (4.2)
  - Participants have and use information and tools to *prevent* fraud to the extent reasonably practicable and legally permissible and feasible (4.3)
  - Participants have and use information and tools to *detect* fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible (4.4)

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."

- **Intended outcomes**:
  - The operator has adopted procedures and practices that support its timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection (5.1)
  - Participants, collectively and individually, have adopted procedures and practices that support their timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection (5.2)

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."

- **Intended outcome**:
  - The operator and participants collaborate in support of information-sharing and ongoing education and awareness about evolving endpoint security risks and risk controls (6.1)

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 obtain potential efficiencies where possible and appropriate. Similarly, regulators, supervisors and overseers of wholesale payment systems and messaging network 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."

- **Intended outcomes**:
  - The operator monitors evolving endpoint security risks and risk controls (7.1)
  - Participants, collectively or individually, monitor evolving endpoint security risks and risk controls (7.2)
  - The operator and, to the extent practicable, participants seek to coordinate approaches for strengthening endpoint security with other relevant systems and networks where possible and appropriate (7.3)
  - The expectations and assessment programmes of regulators, supervisors and overseers of the operator reflect, as appropriate, the relevant intended outcomes of this strategy (7.4)
  - The expectations and assessment programmes of the regulators, supervisors and overseers of the participants reflect, as appropriate, the relevant intended outcomes of this strategy (7.5)

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Key document 5

Intended outcomes and example emerging practices to operationalise the strategy

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Intended outcomes and example emerging practices to operationalise the strategy

Introduction

The CPMI report on reducing the risk of wholesale payments fraud related to endpoint security presents a comprehensive strategy to reduce this risk. The CPMI report also describes a set of actions that the CPMI and each CPMI central bank are now taking to promote and to monitor progress in operationalising the strategy in their institutions and jurisdictions.

As part of this effort to operationalise the strategy, the CPMI has begun collecting examples of "emerging practices" for achieving the intended outcomes of each of the seven elements of the strategy. In order to aid non-CPMI member central banks in their efforts to promote and to operationalise the strategy in their respective institutions and jurisdictions, the CPMI is making this current collection of emerging practices publically available as part of this "toolkit".

It is important to highlight that this current collection of emerging practices should be treated as a "living document" and a non-exhaustive list. As additional examples of practices for achieving the intended outcomes of the strategy are identified, the CPMI intends to include these in future versions.

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."

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 1.1 The operator takes into consideration the range of risks that the individual endpoints of its system pose to the collective confidence in the integrity of the system/network itself **IO 1.2** Participants are aware of the range of risks that individual endpoints of the system pose to their collective confidence in the	**EP 1.1** The operator conducts a formal, annual assessment to identify endpoint security risks. The assessment explicitly takes into consideration the risk of participants and other stakeholders losing confidence in the integrity to the overall system. **EP 1.2** The operator uses external vendors to help with the identification of endpoint security risks and penetration testing.

integrity of the system/network itself	**EP 1.3** The operator engages with regional payment system bodies to identify and understand cross-cutting endpoint security risks. **EP 1.4** The operator has procedures to report internally potential fraud attempts or incidents of unauthorised transactions to inform and support its evolving risk management. **EP 1.5** The operator has an ongoing process to raise and maintain participant awareness of the importance of endpoint security through workshops, seminars and related communication channels. **EP 1.6** Relevant stakeholders in the system/network (eg, the central bank, the operator, participant/user groups) employ communication channels (eg notices, letters, meetings, speeches, educational workshops, conference presentations) to explain and emphasise the need for collective and coordinated action to address the risk of losing confidence in the integrity of the overall system/network.

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

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 2.1 The operator has established requirements for its participants to prevent fraud **IO 2.2** The operator has established requirements for its participants to detect attempted fraud **IO 2.3** The operator has established requirements for its participants regarding their	**EP 2.1** The operator has established requirements for participants to prevent and detect fraud with respect to each participant's endpoint hardware, software, physical access, logical access, organisation and processes. **EP 2.2** The operator encourages or requires participants to use available information and/or tools to prevent fraud by identifying and blocking in "real-time" potentially fraudulent payments before they are sent (see also element 5). **EP 2.3** The operator encourages or requires participants to adopt an explicit framework to detect potential fraud (eg by

immediate response to potential fraud **IO 2.4** The operator has established requirements for its participants, when appropriate, to alert the broader payments network community to evolving fraud threats **IO 2.5** Participants conduct reviews to determine what, if any, supplemental risk-based endpoint security arrangements they may need to establish for themselves	receiving and checking ex post "out of band" reports of sent payments and notices of changes to participant access credentials) (see also element 4). **EP 2.4** The operator encourages or requires participants to use pre-defined procedures and practices (including contact information) for their timely initiation of, and immediate response to, a request to take action concerning a potentially fraudulent payment instruction (including during off-hours) (see also element 5). **EP 2.5** The operator encourages or requires participants to alert the broader payments community to evolving threats and risks (eg via the operator, the participants' supervisors, or the relevant ISACs) (see also element 6). **EP 2.6** The operator's requirements (ie, for preventing fraud; for detecting fraud; for the immediate response to fraud; and for alerting the broader payments network community to evolving fraud threats) are established explicitly in system/network rules.

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."

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 3.1 Processes exist to promote participants' adherence to their respective endpoint security requirements	**EP 3.1** The operator requires each participant to self-attest at least annually to the participant's adherence to the security requirements of operators. **EP 3.2** The operator requires an independent institution to carry out mandatory compliance assessments on participants. **EP 3.3** Participants are required to conduct self-assessments of adherence to established requirements at least annually with the help of an independent third party to provide a review. **EP 3.4** The operator has established incentives for participants to adhere to established requirements (eg by establishing a process for the review of self-attestations/monitoring questionnaires by counterparties, internal/external auditors, supervisors, or other relevant stakeholders). **EP 3.5** The operator has established rules, procedures and processes for participants to address identified endpoint security weaknesses, for example by (i) requiring remediation plans; (ii)

	providing to or agreeing with the participant an appropriate time frame for remediation, with the potential of limiting the participant's access to the system in the event of insufficient remediation; and (iii) reporting a participant's insufficient adherence to the participant's direct supervisory authority. **EP 3.6** Participants are required to adhere to established requirements and to put in place mechanisms to review, identify and remedy any potential gaps in adherence. **EP 3.7** The expectations and assessment programmes of the participants' supervisors reflect, as appropriate, all relevant endpoint security requirements applicable to participants (see also element 7).

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."

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 4.1 The operator has and uses information and tools to prevent fraud to the extent reasonably practicable and legally permissible and feasible **IO 4.2** The operator has and uses information and tools to detect fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible **IO 4.3** Participants have and use information and tools to prevent fraud to the extent reasonably practicable and legally permissible and feasible **IO 4.4** Participants have and use information and tools to detect fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible	**EP 4.1** The operator uses information and tools to prevent fraud by identifying and, with relevant participant's consent/involvement, blocking in "real-time" potentially fraudulent payments before they are processed. This includes (i) tools to authenticate and prevent settlement of anomalous transactions, (ii) tools to block fraudulent transactions submitted and awaiting settlement on instruction, (iii) allowing participants to set "whitelists" of other participants who can be sent funds, (iv) automated fraud intelligence sharing with participants. **EP 4.2** The operator uses information and tools to detect fraud by identifying and investigating, in a timely manner, potentially fraudulent payments that may have been processed. **EP 4.3** Participants use information and tools (either developed internally or provided externally by the operator or a third party) to prevent fraud by identifying and blocking in "real-time" potentially fraudulent payments before they are sent, on the basis of parameters set by participants (eg, to restrict outgoing payments above a certain amount, or to certain payees, or that are intiated outside certain hours).

	EP 4.4 Participants use information and tools (eg ex-post "out of band" reports of sent payments and notices of changes to access credentials provided by the operator) to detect fraud by identifying and investigating in a timely manner potentially fraudulent payments that may have been sent. **EP 4.5** The operator provides tools to participants for identifying and blocking outgoing payments in "real time" with the most restrictive settings predefined and selected by the operator for each participant. Each participant then has the ability to adjust the settings of the tools based on its own activity and judgment. **EP 4.6** The operator and participants take a risk-based approach to using information and tools to prevent and detect potential fraud, such as by focusing on the identification and blocking in "real time" of potentially fraudulent payments sent by smaller system participants and correspondent banking clients.

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."

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 5.1 The operator has adopted procedures and practices that support its timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection **IO 5.2** Participants, collectively and individually, have adopted procedures and practices that support their timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection	**EP 5.1** The operator has developed 24x7 emergency hotlines and contact lists (for itself and its participants), along with internal procedures, tools and staff training programmes, to enable the operator to block pending payments that are identified by itself or its participants as potentially fraudulent. **EP 5.2** Participants have developed 24x7 emergency hotlines, contact lists and internal procedures, tools and staff training programmes, to enable each participant to initiate and to respond to requests to block pending payments that are identified by itself, the operator, or other participants as potentially fraudulent. **EP 5.3** The operator and participants have considered the potential need for, and where necessary have developed, indemnity agreements to support their timely response to

	requests to take action without unduly shifting or creating legal liability. **EP 5.4** Participants actively engage in industry groups to develop best practices for timely fraud response. **EP 5.5** The operator and participants employ industry-wide table top scenario exercises to identify and address potential barriers to a speedy response to fraud.

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."

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 6.1 The operator and participants collaborate in support of information-sharing and ongoing education and awareness about evolving endpoint security risks and risk controls	**EP 6.1** The operator conducts outreach to participants and promotes information-sharing efforts that connect different industry groups (eg banks and credit unions). **EP 6.2** The operator and participants leverage existing cyber security working groups to incorporate fraud-related elements of the strategy into their plans. **EP 6.3** The operator and participants leverage existing national bodies and industry groups and other information exchange mechanisms (eg information-sharing and analysis centres (ISACs)) to share information and to create awareness of evolving risks and risk controls. **EP 6.4** Existing industry information sharing organisations are leveraged by participants to voluntarily alert the broader payments network community to evolving fraud threats. **EP 6.5** The operator and participants have jointly determined how best to share information given the relevant legal constraints related to privacy/data protection and other sensitivities. **EP 6.6** The operator provides informative reports, training sessions, roundtables and other forms of education about evolving risks and risk controls to participants through various means.

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 obtain potential efficiencies where possible and appropriate. Similarly, regulators, supervisors and overseers of wholesale payment systems and messaging network 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."

Intended outcomes (IOs) identified to monitor and assess progress:	Initial set of emerging practices (EPs) identified to help achieve the intended outcomes:
IO 7.1 The operator monitors evolving endpoint security risks and risk controls **IO 7.2** Participants, collectively or individually, monitor evolving endpoint security risks and risk controls **IO 7.3** The operator and, to the extent practicable, participants seek to coordinate approaches for strengthening endpoint security with other relevant systems and networks where possible and appropriate **IO 7.4** The expectations and assessment programmes of regulators, supervisors and overseers of the operator reflect, as appropriate, the relevant intended outcomes of this strategy **IO 7.5** The expectations and assessment programmes of the regulators, supervisors and overseers of the participants reflect, as appropriate, the relevant intended outcomes of this strategy	**EP 7.1** The operator regularly interacts with threat intelligence organisations, both commercial and governmental, to report and to receive updates regarding endpoint security incidents. **EP 7.2** Participants interact, to the extent practicable, with threat intelligence organisations, both commercial and governmental, to report and to receive updates regarding endpoint security incidents. **EP 7.3** The operator regularly engages with participants to report and to receive updates regarding endpoint security incidents. **EP 7.4** The operator engages and exchanges information with other operators on evolving endpoint security approaches, both bilaterally and through multilateral operator groups. **EP 7.5** Participants engage and exchange information on their respective evolving endpoint security approaches through various domestic and international industry groups. **EP 7.6** The central bank has informed the operator's relevant authority (ie, regulator/supervisor/overseer) of the strategy and its intended outcomes, to support the authority's review and updating of its endpoint security expectations and assessment program, as appropriate. **EP 7.7** The central bank has informed the participants' relevant authorities (ie, regulators/supervisors/overseers) of the strategy and its intended outcomes, to support the authorities' review and updating of their endpoint security expectations and assessment programs, as appropriate.

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Key document 6

Template to monitor progress in operationalising the strategy

Committee on Payments and
Market Infrastructures

BANK FOR INTERNATIONAL SETTLEMENTS

Template to monitor progress in operationalising the strategy

Introduction

The CPMI report on the strategy to reduce the risk of wholesale payments fraud related to endpoint security describes a set of actions that the CPMI and its members are taking to promote and to monitor progress in operationalisation of the strategy. This template has been created and used by CPMI member central banks in support of their monitoring and assessments of progress in their respective jurisdictions and their reporting of the results to the CPMI.

Since the launch of the strategy the CPMI has been reaching out to non-CPMI central banks to promote the strategy in the global central bank community. This generic version of the monitoring template has been prepared for central banks and relevant associations/forums of central banks to support and promote the strategy and to monitor progress in their jurisdictions.

Instructions

1. All responses should reflect the information, understanding, and/or judgment from a policy or oversight/supervisory perspective of each central bank that is monitoring progress in its jurisdiction. It may be (and often is) solely within the direct responsibility or authority of other relevant parties, within or outside of the central bank, to operationalise particular aspects of the strategy (eg operators, participants, and bank supervisors). Even in such cases, it is still the central bank in its capacity of promoting and monitoring progress who is responsible for filling out the template and for the accuracy of the reported information, as well as for all judgments and projections. Each central bank is free to request whatever information it deems relevant, and to obtain that information, from whatever source it deems relevant (eg by asking the operator, the participants, their supervisors etc).

2. A separate template should be filled out for each wholesale payment system that the central bank operates, regulates, supervises and/or oversees in its jurisdiction and, where they exist, for each separate stand-alone messaging network in its jurisdiction.

3. To the extent that a wholesale payment system uses a third-party or outsourced messaging network as part of its communications/operations, the combined use should be treated as a "single" payment system in which the relevant usage of the messaging network is just one component part. When taking this approach there is no need to fill out a separate template for that third-party/outsourced messaging network. Instead, please provide a brief description of the operational, governance and other arrangements of the combined use, as relevant.

4. For each aspect of the strategy, the central bank is asked to provide examples of key practices in place and/or potential actions identified and/or being operationalised and, where relevant, any key obstacles or challenges to achieving the intended outcome. To assist respondents in determining which examples to highlight, the template gives some examples of practices/actions that might (and might not) support the intended outcomes of the strategy as well as some considerations for consistency of responses. A more expansive discussion of how different

outcomes can complement and reinforce one another is included in an Annex. The examples and considerations are included as an aid and are not comprehensive or necessarily relevant for every system or jurisdiction.

5. For each aspect of the strategy, the central bank is then asked to describe, supported by the examples provided according to the instruction above, the current state of operationalisation by using the following definitions and by ticking a box of the stage whose definition best describes the state.

State of operationalisation	**Definition**
☐ Stage 0	The central bank has not yet begun to assess whether the intended outcome has been achieved to the extent necessary and practical by all relevant parties, or whether actions needed to achieve it have been adequately identified by the parties that are in the best position to operationalise them.
☐ Stage 1	The central bank is in the process of assessing whether the intended outcome has been achieved to the extent necessary and practical by all relevant parties, and, if it has not, the central bank is in the process of assessing whether actions needed to achieve it have been adequately identified by the parties that are in the best position to operationalise them.
☐ Stage 2	The central bank has determined that actions needed to achieve the intended outcome to the extent necessary and practical have been adequately identified by all relevant parties, and that the parties that are in the best position to operationalise them are in the process of doing so in a timely manner.
☐ Stage 3	The central bank considers that the intended outcome has been achieved to the extent necessary and practical by all relevant parties.
☐ Stage 4	The central bank considers that the intended outcome has been achieved to the extent necessary and practical by all relevant parties. The central bank is also satisfied that all relevant parties have an approach in place to assess whether the intended outcome is maintained continuously over time to the extent practical in light of evolving risks, technology, information, and other developments, and to operationalise further improvements as may be necessary to do so.

6. When assessing and describing the current states of operationalisation, due consideration should be given to not only the existence but also the effectiveness of the practices in place and/or potential enhancements under consideration towards achieving the intended outcome of each aspect of the strategy.

7. Please refer to the CPMI strategy report for terminology explanations. Furthermore, for the purpose of this survey, the term "operator" should be interpreted to include any governing bodies (eg board of directors), senior management, and any other groups or organisations that are responsible for setting any rules, requirements, processes or procedures that apply to the system or network.

8. For the purposes of this survey, the central bank should limit the scope of its answers to its assessment of the wholesale system or messaging network's efforts to address the risk of fraud related to endpoint security, not the risks related to cyber or operational resilience more broadly.

Progress report as of [date]

Name of the monitoring central bank: _____

Name of the system/network: _____

Please provide a brief description of the design and operation of the wholesale payment system or network. In particular, please indicate if the system uses its own proprietary communications/messaging network or one provided by a third party such as SWIFT. Likewise, if applicable and relevant, please list the relevant governing bodies (eg board of directors), senior management, and any other relevant groups or organisations that are outside the system or network and responsible for setting any rules, requirements, processes or procedures that apply to the system or network and its participants, along with a brief explanation of their roles and relationships:

Monitoring template – state of operationalising each aspect of the strategy

Table 1

Reducing the risk of wholesale payments fraud related to endpoint security

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 the endpoint security they face collectively and individually, including risks related to the possible loss of confidence in the integrity of the payment systems or messaging network itself.

Intended outcome	**Key practices/actions to support the intended outcome**	**Assessment of current state**
1.1. The operator takes into consideration the range of risks that the individual endpoints of its system pose to the collective confidence in the integrity of the system/network itself. ***Examples of practices/actions that might support the intended outcome:*** • The operator's risk assessment explicitly takes into consideration the risk of losing confidence in the integrity of the overall system/network. ***Examples of practices/actions that might not be sufficient to support the intended outcome:*** • The operator's risk assessment only focuses on addressing the individual risks faced by operators and participants, such as their individual financial loss and reputational risk without explicitly emphasising the need for collective and coordinated action for a common interest. ***Consideration for consistency:*** • A less advanced state for this outcome is likely to impede progress in others, including outcomes 2.1, 2.2, 2.3, 2.4, 3.1, 4.1, 4.2, 5.1, 6.1, 7.1 and 7.3.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
1.2. Participants are aware of the range of risks that individual endpoints of the system pose to their collective confidence in the integrity of the system/network itself. ***Examples of practices/actions that might support the intended outcome:*** • Communications (eg notices, letters, meetings, speeches, educational workshops, conference presentations) by relevant parties (eg FMI policy makers/overseers, the operator, participants' supervisors) that explicitly	Practices in place and/or actions already taken: • • Practices and/or actions being operationalised: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

emphasise the need for collective and coordinated action among operators and participants to address the risk of losing confidence in the integrity of the overall system/network. ***Examples of practices/actions that might not support the intended outcome:*** • Communications that only focus on addressing the individual risks faced by participants, such as their individual financial loss and reputational risk without explicitly emphasising the need for collective and coordinated action for a common interest. ***Consideration for consistency:*** • A less advanced state for this outcome is likely to impede progress in others, including outcomes 2.5, 4.3, 4.4, 5.2, 6.1, and 7.2.	Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	

2. Establish endpoint requirements

The operator of a wholesale payment system (or messaging network) should be clear about the security requirements of the endpoints for its participants, as part of their participation requirements. Such requirements should include those for prevention and detection, for immediate response and, if necessary, to alert the payments community about the changing threats of fraud. In addition to the requirements established by the operator of a wholesale payment system (or a messaging network), each participant of the payment system (or the messaging network) should identify and establish their own complementary risk-based endpoint security arrangements as needed.

Intended outcome	**Key practices/actions to support the intended outcome**	**Current state**
2.1. The operator has established requirements for its participants to *prevent* fraud. ***Examples of practices/actions that might support the intended outcome:*** • The operator has established requirements for its participants to prevent fraud with respect to each participant's endpoint hardware, software, physical access, logical access, organisation and processes. • The operator encourages or requires participants to use available information and/or tools to identify and to block in "real-time" potentially fraudulent payments before they are sent. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcome 3.1.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

2.2. The operator has established requirements for its participants to *detect* attempted fraud. ***Examples of practices/actions that might support the intended outcome:*** • The operator encourages or requires participants to adopt an explicit framework to detect potential fraud (eg use of ex post reports on "out of band" payments, as pre-defined by each participant, and notices of changes to participant access credentials). ***Examples of practices/actions that might not support the intended outcome:*** • Requirements with respect to a participant's immediate response to potential fraud do not take into consideration a sufficient identification and understanding of the risks, per element 1. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcome 3.1.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
2.3. The operator has established requirements for its participants regarding their immediate *response* to potential fraud. ***Examples of practices/actions that might support the intended outcome:*** • The operator encourages or requires participants to use pre-defined procedures and practices (including contact information) for their timely initiation of, and immediate response to, a request to take action concerning a potentially fraudulent payment instruction (including during off-hours). ***Examples of practices/actions that might not support the intended outcome:***	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• Requirements with respect to a participant's immediate response to potential fraud do not take into consideration a sufficient identification and understanding of the risks, per element 1. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcome 3.1.	•	
2.4. The operator has established requirements for its participants, when appropriate, to alert the broader payments network community to evolving fraud threats. ***Examples of practices/actions that might support the intended outcome:*** • The operator encourages or requires participants to alert the broader payments network community to evolving threats and risk controls (eg via the operator, the participants' supervisors, or the relevant ISACs). ***Examples of practices/actions that might not support the intended outcome:*** • Requirements with respect to alerting the broader payments network community to evolving threats do not take into consideration a sufficient identification and understanding of the risks, per element 1. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcome 3.1.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
2.5. Participants conduct reviews to determine what, if any, supplemental risk-based endpoint security arrangements they may need to establish for themselves. ***Examples of practices/actions that might support the intended outcome:***	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• Participants are encouraged or required (eg by the operator, their supervisor, or as industry practice) to review, and supplement, as needed, the requirements of the system/network operators with their individual endpoint security arrangements to identify and address potential vulnerabilities. ***Examples of practices/actions that might not support the intended outcome:*** • Participant reviews do not take into consideration a sufficient identification and understanding of the risks, per element 1. ***Consideration for consistency:*** • Progress in outcome 1.2 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcome 7.2.	• • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	

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.

Intended outcome	**Key practices/actions to support the intended outcome**	**Current state**
3.1. Processes exist to promote participants' adherence to their respective endpoint security requirements. ***Examples of practices/actions that might support the intended outcome:*** • Participants are required (eg by the operator, their supervisor, or as industry practice) to attest to their adherence to all relevant endpoint security requirements. • Incentives have been established for participants to adhere to requirements (eg via review of self-attestations by counterparties, internal/external auditors, supervisors, or other relevant authorities).	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• The operator has established 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. • Supervisors have reviewed and updated their expectations and assessment programmes, as appropriate, to reflect all relevant endpoint security requirements applicable to participants. ***Examples of practices/actions that might not support the intended outcome:*** • Adherence processes exist, but the requirements themselves may be insufficient (eg, the requirements do not take into consideration a sufficient identification and understanding of the risks, per element 1). ***Consideration for consistency:*** • Progress in outcomes 1.1, 2.1, 2.2, 2.3 and 2.4 is likely to be necessary to achieve a high stage in this outcome.		

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.

Intended outcome	**Key practices/actions to support the intended outcome**	**Current state**
4.1. The operator has and uses information and tools to *prevent* fraud to the extent reasonably practicable and legally permissible and feasible. ***Examples of practices/actions that might support the intended outcome:***	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• In circumstances where it would be reasonably practicable and legally permissible and feasible to do so, the operator is using information and/or tools to identify and, with relevant participant's consent/involvement, to block in "real-time" potentially fraudulent payments before they are processed. ***Examples of practices/actions that might not support the intended outcome:*** • None identified, beyond the lack of practices/actions aimed at achieving the intended outcome. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome.	Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	
4.2. The operator has and uses information and tools to *detect* fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible.***Examples of practices/actions that might support the intended outcome:*** • In circumstances where it would be reasonably practicable and legally permissible and feasible to do so, the operator is using information and tools to identify and to investigate in a timely manner potentially fraudulent payments that may have been processed. ***Examples of practices/actions that might not support the intended outcome:*** • None identified, beyond the lack of practices/actions aimed at achieving the intended outcome. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
4.3. Participants have and use information and tools to *prevent* fraud to the extent reasonably practicable and legally permissible and feasible.	Practices in place and/or actions already taken: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3

Examples of practices/actions that might support the intended outcome: • Participants use information and tools (either developed internally or provided externally by the operator or a third party) to identify and to block in "real-time" potentially fraudulent payments before they are sent. ***Examples of practices/actions that might not support the intended outcome:*** • None identified, beyond the lack of practices/actions aimed at achieving the intended outcome. ***Consideration for consistency:*** • Progress in outcome 1.2 is likely to be necessary to achieve a high stage in this outcome.	Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 4
4.4 Participants have and use information and tools to *detect* fraud in a timely manner to the extent reasonably practicable and legally permissible and feasible. ***Examples of practices/actions that might support the intended outcome:*** • Participants use information and tools (eg "out of band" ex-post payment reports and notices of changes to access credentials provided by the operator) to identify and to investigate in a timely manner potentially fraudulent payments that may have been sent. ***Examples of practices/actions that might not support the intended outcome:*** • Participants have strong endpoint security and cyber intrusion detection practices in place, but they do not use information and tools to identify and to investigate in a timely manner potentially fraudulent payments that may have been sent. ***Consideration for consistency:*** • Progress in outcome 1.2 is likely to be necessary to achieve a high stage in this outcome.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
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.

Intended outcome	**Key practices/actions to support the intended outcome**	**Current state**
5.1. The operator has adopted procedures and practices that support its timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection. ***Examples of practices/actions that might support the intended outcome:*** • The operator has pre-defined procedures and practices, along with accompanying contact information and other necessary resources, that would support its timely response (including during off-hours) to a request from a participant to stop or recall a potentially fraudulent payment without unduly shifting legal liability. ***Examples of practices/actions that might not support the intended outcome:*** • The operator relies on participants to respond to potential fraud without involving the operator. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
5.2. Participants, collectively and individually, have adopted procedures and practices that support their timely initiation of, and response to, a request to take action concerning a potentially fraudulent payment instruction upon detection. ***Examples of practices/actions that might support the intended outcome:***	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• Participants have pre-defined procedures and practices, along with accompanying contact information and other necessary resources, to respond in a timely manner (including during off-hours) to a request to stop or recall a potentially fraudulent payment without unduly shifting legal liability. ***Consideration for consistency:*** • Progress in outcome 1.2 is likely to be necessary to achieve a high stage in this outcome.	• • Key obstacles or challenges to achieving the intended outcome: • • •	

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.

Intended outcome	**Key practices/actions to support the intended outcome**	**Current state**
6.1. The operator and participants collaborate in support of information-sharing and ongoing education and awareness about evolving endpoint security risks and risk controls. ***Examples of practices/actions that might support the intended outcome:*** • The operator and participants leverage national bodies and industry groups or other information exchange mechanisms (eg information-sharing and analysis centres (ISACs) and other user groups) to share information and to create awareness in the industry. • The operator and participants have determined how best to share information given relevant legal constraints related to privacy/data protection and other sensitivities. • Informative reports, training sessions, roundtables and other forms of education are provided to participants through various means. ***Consideration for consistency:*** • Progress in outcomes 1.1, 1.2, 7.1 and 7.2 is likely to be necessary to achieve a high stage in this outcome.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

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.

Intended outcome	**Key practices/actions to support the intended outcome**	**Current state**
7.1. The operator monitors evolving endpoint security risks and risk controls. ***Examples of practices/actions that might support the intended outcome:*** • The operator regularly interacts with threat intelligence organisations, both commercial and governmental. • The operator regularly engages with its participants, including through required reporting by participants of endpoint security incidents. • The operator uses an internal security operations centre (SOC) or forensics team to monitor and analyse threat information. ***Examples of practices/actions that might not support the intended outcome:*** • The operator does not directly monitor evolving endpoint security risks and risk controls and, instead, relies on other system or network operators to do so. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcome 6.1.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
7.2. Participants, collectively or individually, monitor evolving endpoint security risks and risk controls. ***Examples of practices/actions that might support the intended outcome:*** • Participants regularly engage with the operator, including to report and to receive updates regarding endpoint security incidents.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• Participants interact, to the extent practicable, with threat intelligence organisations, both commercial and governmental. ***Examples of practices/actions that might not support the intended outcome:*** • Participants do not directly monitor evolving endpoint security risks and risk controls and, instead, rely on the system or network operator to do so. ***Consideration for consistency:*** • Progress in outcome 1.2 is likely to be necessary to achieve a high stage in this outcome. Likewise, a less advanced state for this outcome may impede progress in outcomes 2.5 and 6.1.	Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	
7.3. The operator and, to the extent practicable, participants seek to coordinate approaches for strengthening endpoint security with other relevant systems and networks where possible and appropriate. ***Examples of practices/actions that might support the intended outcome:*** • The operator engages and exchanges information with other operators on endpoint security approaches both bilaterally and through multilateral operator groups. • Participants engage and exchange information on their respective approaches regarding endpoint security through various domestic and international industry groups. ***Consideration for consistency:*** • Progress in outcome 1.1 is likely to be necessary to achieve a high stage in this outcome.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4
7.4. The expectations and assessment programmes of regulators, supervisors and overseers of the operator reflect, as appropriate, the relevant intended outcomes of this strategy. ***Examples of practices/actions that might support the intended outcome:***	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4

• The central bank has informed the operator's relevant regulator/supervisor/overseer of the strategy and its intended outcomes to support the authority's review and updating of its endpoint security expectations and assessment program, as appropriate.	• Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •		
7.5. The expectations and assessment programmes of the regulators, supervisors and overseers of the participants reflect, as appropriate, the relevant intended outcomes of this strategy. ***Examples of practices/actions that might support the intended outcome:*** • The central bank has informed the participants' relevant regulators/supervisors/overseers of the strategy and its intended outcomes to support the authorities' review and updating of their endpoint security expectations and assessment programs, as appropriate.	Practices in place and/or actions already taken: • • • Practices and/or actions being operationalised: • • • Practices and/or actions identified but not yet being operationalised: • • • Key obstacles or challenges to achieving the intended outcome: • • •	☐ Stage 0 ☐ Stage 1 ☐ Stage 2 ☐ Stage 3 ☐ Stage 4	
Table Note			

Monitoring template – general questions

Reducing the risk of wholesale payments fraud related to endpoint security Table 2

General questions	**Comments:**
A. Please provide a high-level description of your central bank's approach to promoting local progress.	
B. What, if any, significant obstacles to successful operationalisation have been identified in your jurisdiction, and what is the current plan for addressing them?	
C. What, if any, aspects of operationalising the strategy either require or would benefit from cross-system/global coordination/harmonisation? Are you aware of or do you have suggestions for a plan to address this?	
D. What, if any, significant new threats impacting wholesale fraud related to endpoint security have been identified in your jurisdiction, and what is the plan for addressing them?	
E. To what extent if at all, are supervisors of participants of wholesale payment systems and messaging networks identifying as applicable and incorporating as appropriate any of the intended outcomes of the strategy into their supervisory expectations and assessments programmes?	
F. What is your approximate estimate of the timing by when you project Stage 3[1] to be achieved for all aspects of the strategy?	Please choose among: a) end 2020; b) end 2021; and c) other (please specify).

Table Note: 1. Stage 3: The respondent considers that the intended outcome has been achieved to the extent necessary and practical by all relevant parties.

Annex – considerations for consistency

The strategy's seven elements are complementary and reinforce one another. For some intended outcomes, these dependencies and relations are more explicit, and are set out below to act as a prompt for central banks to consider the consistency of reported progress (eg a high stage in outcome 2.2 (i) could be difficult without equivalent progress for 1.1 (dependency) and (ii) is likely to be related to outcomes 2.3 and 2.4 (relationship)).

These potential dependencies and relationships are mapped below. Dependencies are highlighted in green, with a "D" and a greater-than-or-equal-to sign ("≥") denoting in which direction the dependency lies. These should be read upwards, eg outcome 1.1 should be greater than or equal to outcome 2.1. Relationships are highlighted in blue with an "R".

Outcome	**1.1**	**1.2**	**2.1**	**2.2**	**2.3**	**2.4**	**2.5**	**3.1**	**4.1**	**4.2**	**4.3**	**4.4**	**5.1**	**5.2**	**6.1**	**7.1**	**7.2**	**7.3**	**7.4**	**7.5**
1.1	=	R	D≥	D≥	D≥	D≥		D≥	D≥	D≥			D≥		D≥	D≥		D≥		
1.2	R	=					D≥	R			D≥	D≥		D≥	D≥		D≥			
2.1	D≤		=					D≥			R									
2.2	D≤			=	R	R		D≥				R		R	R					
2.3	D≤			R	=			D≥					R							
2.4	D≤			R		=		D≥			R	R								
2.5		D≤					=										D≥			
3.1	D≤	R	D≤	D≤	D≤	D≤		=			R	R		R	R					
4.1	D≤								=						R					
4.2	D≤									=					R					
4.3		D≤	R			R		R			=									
4.4		D≤		R		R		R				=		R	R		R			
5.1	D≤				R								=							
5.2		D≤		R				R				R		=						
6.1	D≤	D≤		R				R	R	R		R			=	D≤	D≤			
7.1	D≤														D≥	=				
7.2		D≤					D≥					R			D≥		=			
7.3	D≤																	=		
7.4																			=	
7.5																				=