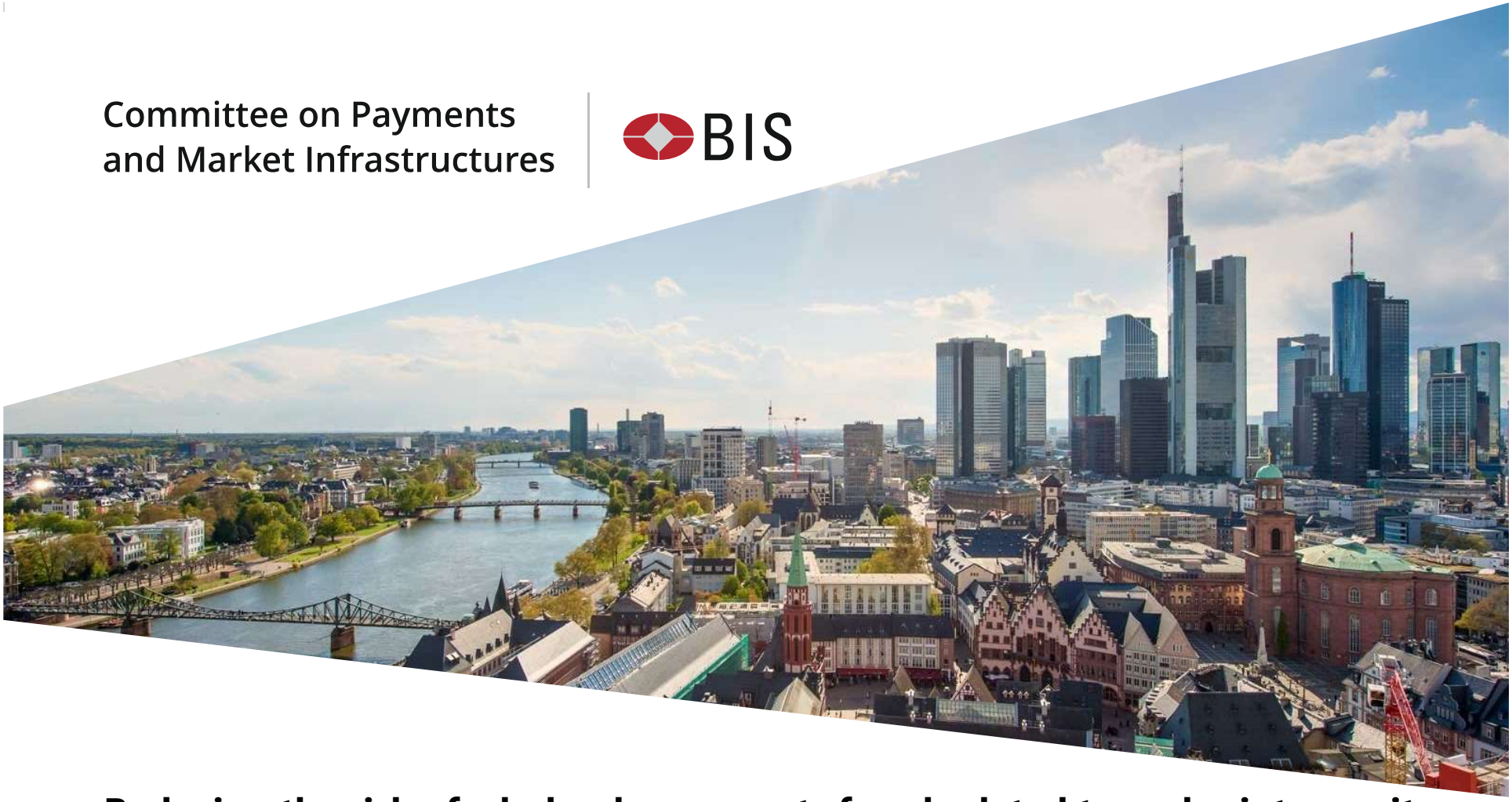
Committee on Payments
and Market Infrastructures

BIS



Reducing the risk of wholesale payments fraud related to endpoint security

Lawrence Sweet

Financial Sector Cyber Resilience Workshop
Mexico City
6-7 November 2019

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
- Next steps in operationalizing the strategy
- Central bank toolkit for operationalising the strategy

Annex1: The seven elements and intended outcomes of the CPMI strategy

Annex 2: Initial set of emerging practices for achieving the intended outcomes

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 Bangladesh Bank and other notable cases, 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 "internalize" 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 operationalizing 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 central banks have teams specifically tasked with promoting and monitoring progress in their 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
    - Global industry workshop held in February to identify and share emerging practices for operationalising the strategy
    - Follow up industry workshop is being planned for December
  - *Promoting awareness and supporting adoption by all central banks around the world*
    - ***Toolkit now available*** *for central banks wishing to operationalise the strategy*

Central bank toolkit for operationalising the strategy

- Identifies and supports steps that central banks could take, such as:
  - Promoting awareness of the risk and the strategy
  - Conducting an initial stock-taking
  - Engaging with relevant stakeholders
  - Developing an action plan
  - Monitoring progress.
- For use by individual central banks, as part of a regional effort, or both
- Key documents are included for each step, including:
  - List of intended outcomes and emerging practices to achieve them
    - Not all practices will be relevant and appropriate for all jurisdictions
    - Can aid central banks in analysing and identifying those to pursue
  - Template for monitoring progress
- The toolkit is a "living document"
  - It will evolve with progress, experience, and emerging practices

Annex 1:

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 assessed in the 2019 CPMI monitoring survey**:
  - 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 assessed in the 2019 CPMI monitoring survey**:
  - 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 outcomes assessed in the 2019 CPMI monitoring survey**:
  - 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 assessed in the 2019 CPMI monitoring survey**:
  - 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 assessed in the 2019 CPMI monitoring survey**:
  - 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 assessed in the 2019 CPMI monitoring survey**:
  - 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 assessed in the 2019 CPMI monitoring survey**:
  - 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)

Annex 2:

Initial set of emerging practices for achieving the intended outcomes of the strategy

Element 1: Identify and understand the range of risks

- 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.
- The operator uses external vendors to help with the identification of endpoint security risks and penetration testing.
- The operator engages with regional payment system bodies to identify and understand cross-cutting endpoint security risks.
- The operator has procedures to report internally potential fraud attempts or incidents of unauthorised transactions to inform and support its evolving risk management.
- 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.
- 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 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.
- 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).
- The operator encourages or requires 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).
- 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).
- 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).
- 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

- The operator requires each participant to self-attest at least annually to the participant's adherence to the security requirements of operators.
- The operator requires an independent institution to carry out mandatory compliance assessments on participants.
- 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.
- 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).
- 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.
- Participants are required to adhere to established requirements and to put in place mechanisms to review, identify and remedy any potential gaps in adherence.
- 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

- 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.
- 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.
- 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 initiated outside certain hours).
- 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.
- 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.
- 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 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.
- Participants have developed 24x7 emergency hotlines, contact lists and internal procedures, tools and staff trainingprogrammes, 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.
- 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.
- Participants actively engage in industry groups to develop best practices for timely fraud response.
- 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 conducts outreach to participants and promotes information-sharing efforts that connect different industry groups (eg banks and credit unions).
- The operator and participants leverage existing cyber security working groups to incorporate fraud-related elements of the strategy into their plans.
- 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.
- Existing industry information sharing organisations are leveraged by participants to voluntarily alert the broader payments network community to evolving fraud threats.
- 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.
- 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 regularly interacts with threat intelligence organisations, both commercial and governmental, to report and to receive updates regarding endpoint security incidents.
- Participants interact, to the extent practicable, with threat intelligence organisations, both commercial and governmental, to report and to receive updates regarding endpoint security incidents.
- The operator regularly engages with participants to report and to receive updates regarding endpoint security incidents.
- The operator engages and exchanges information with other operators on evolving endpoint security approaches, both bilaterally and through multilateral operator groups.
- Participants engage and exchange information on their respective evolving endpoint security approaches through various domestic and international industry groups.
- 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.
- 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.