Specific theme : Endpoint security : a comparative overview of approaches to reduce payment fraud

Filip Caron

Significant developments are apparent in the cyber threat landscape of the global financial industry. Sophisticated adversaries have been acquiring – and successfully exploiting – detailed knowledge on the business processes and IT infrastructure needed to conduct payments. While the 2016 cyber attack against the Bank of Bangladesh was a watershed moment for the industry, a further refining of the cyber attack vectors is being observed. A coordinated community supported response will be needed.

Forensic analysis of recent cyber incidents in the financial sector has indicated that compromising the endpoints of a payment system to inject fraudulent payments, is a viable strategy for cyber criminals. Sophisticated custom malware has been used to acquire administrator rights, manipulate software in memory, bypass authentication mechanisms, install process monitoring tools and delay incident response by hiding evidence and installing ransomware as a smokescreen.

Recurring payment fraud may expose the ecosystem to risks that have an impact far beyond the financial losses for a compromised endpoint ; it may undermine confidence in the integrity of the payment infrastructure. Participants with concerns about the integrity of the system or the implications for their own security posture may be tempted to implement controls that further limit payment instruction processing. In a worst-case scenario, these controls could impede economic activity and even threaten financial stability in the case of wholesale payments.

For this article, an endpoint of a payment system, service provider or network is defined as a point in place and time at which payment instruction information is exchanged between parties and their respective information systems. The next section introduces the three established endpoint security initiatives, followed by a comparative analysis of these initiatives in various dimensions. The concluding section discusses the findings and puts forward significant challenges related to the operationalisation of these strategies.

Endpoint security approaches to reduce payments fraud

A wide spectrum of payment arrangements exists in the financial industry, each with a different infrastructural set-up and security needs. Three diverse initiatives that aim to get a grip on endpoint security to reduce payment fraud have received close attention.

– SWIFT's Customer Security Programme (SWIFT's CSP) targeting security among participants of its messaging and network services ;

– The Payment Card Industry Data Security Standard (PCIDSS) developed by the major card schemes (i.e. American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.) to establish a data security baseline for all entities involved in payment card processing or the storage, processing or transmission of cardholder data and/or sensitive authentication data;
– Security-related specifications under the Second Payments Services Directive (PSD2), which set security baselines for *payment initiation service providers* (PISP) and payers, and endpoints for the systems of *account servicing payment service providers* (ASPSP) and PISPs respectively.

Each of the initiatives targets a different segment of the payments market, namely interbank payment messages, card payments and internet payments. While all three initiatives aim at mitigating risks related to information security and loss of confidence, there is a financial stability risk dimension for the wholesale payments market, as SWIFT is considered a systemically important service provider for the segment.

The three endpoint security reinforcing initiatives are being sponsored by three significantly different stakeholders: an industry incumbent, an industry council and a regulator. While this indicates that a wide variety of stakeholders may be interested in operationalising an endpoint security strategy, it also suggests opportunities for active cooperation with the private sector.

Furthermore, the endpoint infrastructures considered for an endpoint security reinforcing initiative may vary significantly. SWIFT's CSP focuses primarily on the local SWIFT infrastructure (including the operators and their computers) at their participants, as well as the relevant data flows with back office applications. The security-related specifications under PSD2 cover the full infrastructure of the PISP linked via *application programming interfaces* (APIs) to the ASPSP and the strong authentication mechanisms of the payers. Depending on the presence of compensating controls, de facto effective network segmentation, the scope of the PCIDSS either includes the full network-connected infrastructure at the endpoint or is limited to the isolated cardholder data environment (i.e. people, processes and technologies used for the storage, processing and/or transmission of cardholder data or sensitive authentication data).

The Basel Committee for Payments and Market Infrastructures (CPMI) recently presented a general strategy for reducing the risk of wholesale payments fraud related to endpoint security, more details can be found in box 1.

Strategic elements in payment fraud reduction

The comparative analysis of the endpoint security initiatives will focus on four aspects: mechanisms for increasing security baselines for endpoints, mechanisms for promoting the reinforcement of endpoint security, tools for fraud prevention and detection and fraud response procedures. As the validation of PCIDSS compliance may vary depending on the payment card scheme, this comparative analysis is based on MasterCard's approach to endpoint security.

Increasing security baselines for endpoints

Recent cyber incidents revealed important security weaknesses at the endpoints of payment service providers, making them the perceived weakest link in the payment chain and a suitable target for cyber criminals. As a result, improving the security baselines for endpoints could be a viable objective for a payment fraud reduction initiative.

There are various potential options for improving the security baseline for endpoints, including the prescription of hard technical requirements, mechanical enforcement of security enhancements such as automatic mandatory updates, targeted awareness campaigns and principle-based security requirements. Specifying challenging but attainable security requirements has been the preferred option in each of the three initiatives.

Box – CPMI Strategy for reducing the risk of wholesale payments fraud related to endpoint security

In response to the growing threat of wholesale payment fraud, which may undermine confidence in the integrity of the entire system, the Basel Committee on Payments and Market Infrastructures (CPMI) developed a strategy to encourage and help focus industry efforts towards reducing the risk of wholesale payments fraud related to endpoint security.

The **strategy** addresses all areas relevant to payment fraud prevention, detection, response and (external) communication. Seven strategy elements provide a high-level overview of the actions needed.

1. ***Identify and understand the range of risks*** faced by the various actors in the ecosystem, including payment system operators, networks and participants. In addition to security risks faced by individual actors, there are risks faced collectively such as a potential loss of confidence in a payments system;
2. ***Establish endpoint requirements*** that specify a minimum-security baseline for all payment system and network participants;
3. Processes to ***promote adherence*** should ensure that all payment system and network participants comply with the endpoint requirements;
4. ***Provide and use information and tools to improve prevention and detection*** which would enhance the participants' capabilities to prevent and/or detect in a timely manner wholesale payment fraud attempts;
5. Define standardised practices to ***respond in a timely way to potential fraud***;
6. ***Support ongoing education, awareness and information-sharing***;
7. ***Learn, evolve and coordinate.***

While being descriptive and thereby allowing for the necessary flexibility, the CPMI has distilled points for consideration from experienced stakeholders' comments. These points for consideration could assist other operators, participants and relevant stakeholders in developing and operationalising their individual endpoint security strategy.

All stakeholders in the wholesale payment ecosystem should take responsibility for their own systems, risk management and internal control frameworks. Concretely, complying with endpoint security requirements does not imply a shift in liability from participants to wholesale payment system or network operators; participants remain responsible for conducting adequate due diligence assessments of counterparties; and participants adopting fraud prevention and detection tools developed by a payment system or network operator remain responsible for accurately parameterising these tools and dealing with the alerts that they generate.

A successful **operationalisation** of the presented strategy will depend on active cooperation between all relevant actors, including payment system operators, participants and public stakeholders. The CPMI is committed to promoting effective and coherent operationalisation of the strategy within and across jurisdictions and systems. CPMI member central banks will act as catalyst for the effective and coherent operationalisation of the strategy within and across jurisdictions and systems, monitor progress throughout 2018 and 2019, and where necessary take action to ensure adequate progress in the operationalisation of the strategy. That action includes encouraging the establishment of responsibilities and timelines, as well as identifying significant obstacles and/or opportunities (e.g. for cross-system coordination or harmonisation). The Cooperative Oversight of SWIFT, and the Bank as the lead overseer, follow up on the implementation of SWIFT's Customer Security Programme, an advanced operationalisation of the strategy.

The strategy is relevant for several risk management topics covered in the CPMI-IOSCO Principles for Financial Market Infrastructures (PFMIs); Annex F of the PFMIs on oversight expectations for critical service providers; and

the CPMI-IOSCO guidance on cyber resilience for financial market infrastructures. The strategy is not intended to replace or supersede them.

References:
- https://www.bis.org/cpmi/publ/d178.htm.
- https://www.nbb.be/nl/artikels/central-banks-urge-industry-wide-take-strategy-improve-wholesale-payments-security.

The security requirements in the three initiatives, which together form the security baseline for endpoints, are generally well grounded in internationally accepted information security standards such as the ISO/IEC 27002 and the NIST Cybersecurity Framework. Control objectives are adapted to the endpoint security context and cover the prevention of payment fraud (e.g. effective network segregation, strong access control, system hardening, penetration testing and security awareness campaigns); the detection of payment fraud (e.g. implementation of intrusion detection systems, software/data base integrity checking and payments control); and response to detected payment fraud (e.g. specifying incident response plans). While the actual security requirements are relatively comparable across initiatives, the focus varies slightly. Examples of individual focal points include the transmission and storage of critical information in PCIDSS, network segregation in SWIFT's CSP and governance and risk management in the context of PSD2. An overview of the high-level control objectives per initiative can be found in Table 1.

TABLE 1 OVERVIEW OF THE HIGH-LEVEL CONTROL OBJECTIVES

SWIFT's CSP	PCI-DSS	PSD2
1. Restrict internet access & protect critical systems from general IT environment	1. Build and maintain a secure network and systems	1. Governance
2. Reduce attack surface and vulnerabilities	2. Protect cardholder data	2. Risk assessment
3. Physically secure the environment	3. Maintain a vulnerability management programme	3. Protection
4. Prevent compromise of credentials	4. Implement strong access control measures	4. Detection
5. Manage identities and segregate privileges	5. Monitor and test networks	5. Business continuity
6. Detect anomalous activity in systems or transaction records	6. Maintain an information security policy	6. Testing of security measures
7. Plan for incident response and information sharing		7. Situational awareness and continuous learning
		8. Payment service user relationship management
		9. Strong customer authentication
		10. Secure communication

Principle-based specifications of endpoint security requirements are mostly preferred over prescriptive control implementations outlining how a participant should comply with an endpoint security requirement. These principle-based specifications allow participants to design controls that are practical, appropriate and effective given the unique attributes of their system.

All three initiatives claim a principle-based approach; however, the requirements in the PCIDSS tend to be more prescriptive than those formulated by the European regulators in the context of PSD2. For example, the European regulators specify that PISPs should establish and implement preventive security measures against identified operational and security risks (e.g. firewalls), and that these measures should be implemented in a defence-in-depth approach. In contrast, the PCIDSS and SWIFT – respectively in the requirements and implementation guidelines sections – go as far as specifying a maximum interval between the review of firewall rules. Another subtle difference in the requirements of the various initiatives is their level of strictness for a similar level of prescriptiveness. For example, under the PCIDSS the firewall rules need to be reviewed every six months, while SWIFT's guidelines stipulate an annual review.

The initiatives provide for proportionality mechanisms, which might mean a distinction between mandatory and advisory controls or differentiated requirements based on specific characteristics of the endpoints. SWIFT adopted both types of proportionality mechanism in its CSP. While the majority of the 27 security requirements are mandatory, SWIFT proposes 11 best practices as advisory security requirements. Additionally, connectivity aggregators providing access to the SWIFT network for third parties need to comply with both mandatory and advisory controls, in contrast to other customers. PCIDSS provides for additional controls for service providers and entities using specific technologies or infrastructural artefacts (e.g. the encryption protocol SSL/early TLS). Within the context of the PSD2, the European regulators allow for several exemptions from strong customer authentication, e.g. for contactless payments at point of sale, low-value transactions, or payments identified as low risk by a suitable transaction monitoring mechanism.

Promoting the reinforcement of endpoint security postures

Endpoint security requirement specifications should be complemented with adequate processes for ensuring adherence to these requirements. There are many possible approaches, including transparency to various stakeholders, mandatory audits, mechanical enforcement, disconnection, or regulatory requirements.

Transparency on the endpoint security posture of participants aims at creating peer-driven momentum to strengthen endpoint security. Participants can take this information into account when conducting counterparty risk assessments, potentially resulting in additional due diligence activity or counterparty-risk-mitigating measures (e.g. limiting amounts or allowed transaction types). There are various potential approaches to transparency : in a scheme with active transparency, endpoint security information is automatically passed on to all known counterparties, whereas in a scheme with passive transparency, counterparties should request access to this information. Additionally, the sponsor of an endpoint security initiative could establish a process to inform the relevant supervisory authorities of (sustained) endpoint security issues, which may result in supervisory pressure on the non-compliant participant.

Sometimes, adherence to an endpoint security requirement could be achieved through mechanical enforcement. For example, a payment service operator could discard messages sent from an endpoint system that does not support two-factor authentication or has not been patched adequately. In a more extreme scenario, a payment service provider, system or network may even opt to disconnect a participant in the event of sustained non-compliance with the requirements. Mechanical enforcement and disconnection enforcement approaches demand action from the payment service provider, system or network, whereas in a transparency-based approach the stakeholders are requested to make risk-informed decisions.

While mechanical enforcement is always based on evidence collection (i.e. automatic screening or auditing/certification), sponsors of an endpoint security initiative may decide on a self-attestation process to collect information regarding the endpoint security posture of a participant. The latter can be complemented with assurance reports from internal and/or external security auditors.

SWIFT has opted for a peer-driven transparency model and requests its users to self-attest on an annual basis. Participants could demand – on a peer-to-peer basis – access to the endpoint security self-attestation of their counterparties. Furthermore, SWIFT has reserved the right to inform relevant supervisory authorities on self-attestation information.

PISPs must provide their competent authority with regular assessment of both the operational and security risks related to their service and the adequacy of the risk mitigation measures. Article 95(2) of the PSD2 prescribes that these assessments will be provided on an annual basis or at shorter intervals if specified by the competent authority. Regarding the link between PISPs and their endpoints, the regulatory technical standard on strong customer authentication and secure communication stipulates that the relevant security measures should be periodically tested and audited by operationally independent IT experts. Audit reports should be provided to the competent authorities upon their request.

While the PCI Security Standards Council (PCI SSC) is responsible for maintaining the PCIDSS and related programmes (including the assessment training and programmes), the enforcement mechanisms are specific to each payment card scheme. Depending on the type of endpoint (primarily driven by the number of transactions), MasterCard requires annual onsite assessments or annual self-assessments (under certain circumstances with transparency towards acquiring institutions). In addition, quarterly network scans by external providers of tested and PCI approved vulnerability scanning services are required.

Designing methods for payment fraud prevention and detection

Fraud prevention and detection tools could further reduce the likelihood and impact of payment fraud. The tools envisaged by the sponsors of the endpoint security initiatives can be divided into four broad categories: reconciliation, strong authentication, statistical analysis, and artificial intelligence applications.

Recent cyber incidents clearly indicated the popularity of transaction log manipulation to conceal payment fraud. Reconciliation tools allow for detecting manipulations of the transaction logs based on independent reports delivered through a separate and secure channel to an endpoint. SWIFT developed the Daily Validation Reports service, which targets smaller participants interested in validating wholesale payments recorded in an endpoint-local transaction database. Certain payment service providers provide similar tools for their respective endpoints, e.g. Worldline offers its participant merchants a reconciliation mechanism as part of its commercial acquiring services.

Strong authentication of an endpoint operator is based on two or more authentication factors, including knowledge factors such as a password; possession factors like owning a token or specific mobile phone number; and inherence factors which are typically biometrics. While there is a significant list of exemptions, PSD2-related security regulation prescribes per default the need for strong authentication. Payment card schemes actively support strong authentication mechanisms. For example, MasterCard requests its issuers to support EMV 3-D Secure 2.0 by the end of 2018, which should be used by its merchants by the end of 2020. SWIFT imposes multi-factor authentication through a mandatory security requirement.

Statistical analysis tools use metrics and related thresholds – formalised in payment policies – to identify potential fraudulent payments. Typical metrics are based on (combinations of) the payment amount, the beneficiaries, and/or the timing/location of the payment instruction's initiation. SWIFT announced a payment control service that allows endpoint operators to specify a payment policy and determine the actions to be taken in the event of an out-of-policy payment instruction. If effective transaction risk analysis is implemented, payment service providers may be exempted from the strong authentication security requirement under PSD2.

Artificial-intelligence-based tools use a variety of recorded data points and expert knowledge to flag potentially fraudulent payments. The algorithms behind MasterCard's Decision Intelligence service examine cardholder behaviour to detect abnormal behaviour and provide a risk score to the issuer. This risk score could influence an issuer's decision to authorise a transaction. As of July 2018, MasterCard will mandate its issuers to enable a transaction alert service that warns cardholders of the potentially fraudulent use of their card. Acquirers are recommended to opt for a merchant monitoring solution to avoid the processing of illegal and brand-damaging transactions. It should be noted that endpoint operators in the various initiatives can always complement mandated tools with a series of other commercially available data analysis tools to enhance their fraud detection.

Given the complexity of these payment fraud detection and prevention tools, there may be a strong incentive to develop them in collaboration with other stakeholders in the ecosystem. For example, MasterCard's Decision Intelligence is a standardised service used by a variety of issuers. Furthermore, fraud detection tools might have specific data requirements that cannot be satisfied by everyone. Reconciliation tools are typically provided by the payment service, system or network operator as they are based on the formal transaction records of that operator (e.g. SWIFT's Daily Validation Reports), which are typically not accessible to other third-party vendors.

Responding to security incidents and payment fraud attempts

Standardised processes and practices to respond to actual or suspected fraud – in a timely manner – should be defined. The objective of these processes should be three-fold, i.e. specifying reporting mechanisms, developing operational responses and distilling actionable cyber intelligence to protect other endpoints.

The regulatory guidelines on major incident reporting under PSD2, addressed to PISPs, specify the criteria, thresholds and methodology to classify operational and security incidents. If an incident is classified as severe, it needs to be reported to the competent domestic authorities using a standardised template within specified timeframes. Furthermore, these guidelines prescribe the criteria that competent domestic authorities could consider in assessing the incidents' relevance

to other authorities and the detail that needs to be shared. Where relevant, cooperation will be promoted between the competent authorities and the EU Agency for Network and Information Security (ENISA).

SWIFT and MasterCard have specified contractual obligations regarding the reporting of security incidents. These contractual obligations cover the preservation of evidence, execution of forensic analyses, and reporting of incidents and findings. Furthermore, standardised procedures to mitigate the loss of individual fraudulent payments have been developed. SWIFT's Standards MT Release 2018 makes it mandatory to include a unique end-to-end tracking (UETR) number in the header of a FIN message. Originally introduced as part of the Global Payment Innovation (GPI) initiative for tracking payments in a payment chain, the UETR enables the establishment of a stop-and-recall procedure (to be launched in 2018). Payment card schemes have standardised rules for fraud-related chargebacks at acquirer and merchant level, which are enforced through both fines and the threat of cancellation of merchant accounts and acquiring licences.

Forensic analysis of security incidents and payment fraud attempts may result in cyber intelligence such as indicators of compromise and attack vectors. Under its CSP, SWIFT established a customer security intelligence team that assists affected customers with forensic investigations. Distilled cyber intelligence is further distributed in SWIFT's community through a dedicated information sharing and analysis centre (ISAC).

Conclusion

The high degree of interconnectedness between financial information systems has been identified as a significant driver of operational, cyber and reputation risk for the operators of individual systems. Connected IT systems at partners are typically not managed by the financial information systems operators, and have proven to be the weakest link in recent cyber incidents involving payment fraud.

Technology risk managers increasingly focus on developing endpoint security initiatives. These initiatives allow for promoting stronger cyber security across all stakeholders, pooling efforts to develop effective payment fraud detection mechanisms, and defining a standardised approach to ensure an effective response to payment fraud.

The comparison of the various initiatives identified a general recurring structure consisting of specifying security requirements, promoting adherence to these requirements, endorsing the use of fraud prevention/detection mechanisms, and prescribing a standardised fraud response. However, different options to operationalise the endpoint strategies have been chosen. A summary can be found in Table 2.

The operationalisation of endpoint security initiatives still faces significant challenges. Stakeholders may fall within the scope of different endpoint security initiatives with conflicting endpoint security requirements. As self-attestation – and the expected peer pressure of transparency on compliance – remains the favourite security requirement adherence promotion method, each stakeholder has to accept its own responsibility. Restrictions concerning data sharing, privacy and law-enforcement may hamper the efficient sharing of cyber threat intelligence. Endpoint security initiatives will have to be carefully reviewed and peer-revised promptly to remain effective in the continuously evolving threat landscape.

TABLE 2 COMPARISON OF THE ENDPOINT SECURITY INITIATIVES

Endpoint security initiative	SWIFT's CSP	PCI-DSS	PSD2
Sponsor	Wholesale payment messaging service and network operator SWIFT	Card payment schemes grouped in the PCI Security Standards Council	European regulators
System-endpoint relationships covered	• SWIFT – SWIFT participants (including financial institutions, corporates and other organisations)	• Acquirer – Merchant • Issuer – Customer • Card scheme – Acquirer • Card Scheme – Issuer • Relationships with third party service providers (e.g. network operators like Worldline, data process and/or storage service providers)	• ASPSP – PISP • PISP – payers
Mechanisms for increasing security baselines for endpoints	• Principle-based security requirements • Advisory controls	• Principle-based security requirements	• Principle-based security requirements formalised in regulation
Mechanisms for promoting the reinforcement of endpoint security	• Self-attestation • Passive transparency to counterparties • Reporting to regulators • SWIFT retains a right to audit	Depending on the payment card scheme and certain parameters, the following mechanisms may be mandatory: • Self-assessment • Annual onsite assessments • Quarterly network scans	• Self-assessments to be provided to the competent supervisory authorities • Mandated periodic testing of security measures • Mandated regular audits by independent IT experts
Tools for fraud prevention and detection	• Included as an advisory control (multi-factor authentication mandatory) • SWIFT specific services offered	• Implementation is mandatory for issuers and acquirers • Payment scheme specific tools and variety of third-party tool providers	• Strong authentication mandatory • Transaction risk analysis might result in exemptions
Fraud response procedures	• Reporting contractually obligatory • Forensic analysis supported by Customer Security Intelligence team at SWIFT • Stop-and-recall mechanism in GPI • Dedicated ISAC	• Reporting, preservation of evidence and forensic analysis may be contractually obligatory for a card scheme	• Strict reporting guidelines • Sharing beyond local authorities under predefined circumstances