SWIFT's response to the European Banking Authority's Consultation Paper on "Draft Guidelines on the security measures for operational and security risks of payment services under PSD2"

SWIFT

01 August 2017

Confidentiality: Public

SWIFT thanks the European Banking Authority for the opportunity to provide comments on the Consultation Paper Draft Guidelines on the security measures for operational and security risks of payment services under PSD2.

SWIFT is a member-owned cooperative headquartered in Belgium. SWIFT is organised under Belgian law and is owned and controlled by its shareholders, comprising over 2,400 financial institutions. We connect more than 11,000 connected firms, in more than 200 countries and territories. A fundamental tenet of SWIFT's governance is to continually reduce costs and eliminate risks and frictions from industry processes.

SWIFT provides banking, securities, and other regulated financial organisations, as well as corporates, with a comprehensive suite of messaging products and services. We support a range of financial functions, including payments, securities settlement, reporting, and treasury operations. SWIFT also has a proven track record of bringing the financial community together to work collaboratively, to shape market practice, define formal standards and debate issues of mutual interest.

If you wish to discuss any aspect of our response please do not hesitate to let us know.

Natasha de Terán
SWIFT | Head of Corporate Affairs
Tel: + 44 20 7762 2151
Mob: + 44 7780 483 467
www.swift.com

Stefano Ciminello
SWIFT | Deputy CISO
Tel: + 32 2 655 3111
www.swift.com

Introduction

SWIFT supports EBA's proposal for Guidelines on the security measures for operational and security risks of payment services. We believe it is in the financial industry's best interest and in particular to Payment Service Providers (PSPs) to implement high levels of security hygiene and implement measures to address cybersecurity threats. SWIFT has recently published its Customer Security Controls Framework, a series of mandatory and advisory controls with accompanying implementation guidelines for the SWIFT community to adopt.

These controls reflect good security practice and are intended to help customers to safeguard their local environments and reinforce the security of the global financial community. The controls have been developed based on analysis of the latest cyber-threat intelligence resulting from detailed analysis of customer security incidents, but they should also apply beyond customers' SWIFT-related infrastructure into the broader end-to-end transaction chain. The controls were designed in conjunction with industry experts and, prior to the finalisation of the Framework, were subject to extensive review across market segments and through SWIFT's regulatory oversight process. Whilst some of the details underpinning the controls are SWIFT-specific, we feel that the majority would apply in non-SWIFT environments.

We have therefore compared the detail of the proposed measures to the SWIFT Customer Security Control Framework. We believe there are a number of areas in which, on the basis of evolving best practice, the EBA may wish to consider augmenting the proposed measures beyond those currently set out. Our comments below follow the structure of the consultation document.

Guideline 3: Protection

Data and Systems Integrity and Confidentiality

Within PSPs IT production environments there are subsets of critical systems which may warrant the deployment of additional security controls. These subsets are likely to include the physical points from which payment instructions are generated before being transmitted into external networks. Such critical systems may benefit from being grouped in a "secure zone" where, in line with the "layered approach" mentioned in the consultation, additional controls are then employed. These additional controls could include:

- Segregation via physical, network and logical security;
- Restriction of internet access;
- System hardening to reduce the "attack surface" for cyber related events.

The above should be considered for any PSP production environment as best practice controls. However, for critical systems within the PSP production environment SWIFT recommends making these controls mandatory

Separately, we note that no measure is proposed regarding the password policy which PSPs should implement across their systems both for internal and end users. We believe the EBA's measures would benefit from such a control being present. Such a policy should then be reviewed on a regular basis to ensure it continues to evolve with best practice.

Access Control

SWIFT fully supports the EBA's proposed measures for privileged system access. There is, however, one area in which we believe the proposed measures could be further reinforced – namely around the "native" Privileged/Administrator accounts that systems are shipped with.

We believe that the EBA’s measures could be strengthened by restricting the use of and access to these accounts as much as possible. This is of particular importance, given the breadth of access that Privileged systems often provide. Such “native” Privileged/Administrator accounts should only be used on a “break-glass” emergency basis and when full controls over access and usage monitoring are present, while individually accountable controlled accounts with sub-sets of appropriate privileged capabilities should be created wherever possible. This will ensure that appropriate and controlled corrective actions can be taken to address system issues without exposing entire systems to risk. Linked to this is the need to logically and physically protect the passwords for Privileged/Administrator accounts. If stored by logical means, they should not be stored in plain text and appropriate encryption should be employed. If stored physically, these should be stored in a protected environment which meets recognised protection standards. In both instances, appropriate authenticated and recording/monitoring mechanisms should be deployed to control access to the passwords.

SWIFT strongly supports the statement made in Section 3.12 on the use of strong authentication to reduce the risk associated with remote administrative access. We suggest the statement be enhanced to specify the need for Multi-Factor Authentication. This would reflect the criticality of such facilities and the need to strongly control access to them. We believe such access has the same risk profile as ‘*payment initiation and other fraud-inducing actions through a remote channel*’ defined in PSD2 and would therefore also require multi-factor authentication as per EBA’s recently published final “Draft Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication”.

Guideline 4: Detection

Continuous monitoring and detection

SWIFT strongly supports the proposal to continuously monitor and detect anomalous activities, in particular the suggestion that this should cover transactions as well as threats, such as unauthorised intrusions. For PSPs, we would recommend that this should be further strengthened so that transaction activity is restricted to validated and approved counterparties, and that steps are taken to validate whether transactions are within the expected bounds of normal business (for example, within the normal patterns of timing, beneficiaries and value size). Exceptions to this should ideally be flagged in real time, monitored and tracked and transactions should remain in a pending status whilst investigations are completed. Recent events have highlighted the value of such controls being in place.

Additionally, we would recommend that PSPs might perform extra reconciliation checks against external sources as a further check whether their own systems have been compromised.

--- END OF DOCUMENT ---