SWIFT Response to the Committee on Payments and Market Infrastructures discussion note:

“Reducing the risk of wholesale payments fraud related to endpoint security”

28 November 2017

SWIFT thanks the Committee on Payments and Market Infrastructures (the Committee) for the opportunity to provide comments on the discussion note "Reducing the risk of wholesale payments fraud related to endpoint security".

As the Committee observes, the increasing severity of the cyber threat, and the growing sophistication of cyber actors requires an increased level of focus by all participants and public sector stakeholders, particularly in the payments area. We strongly support the Committee's focus on this important matter, and applaud the fact that the Committee is taking a multi-stakeholder approach in this consultation, involving both public and private sectors. While global cooperation is of course key to protecting against any cyber threat, the intrinsically interconnected and international nature of the payments market and its participants makes it especially important that a holistic approach is taken to counter this particular threat. Furthermore consistency and strong coordination across jurisdictions is critical. For these reasons, we believe the Committee's leadership and work in this area is vitally important, and we look forward to the eventual publication of this globally accepted guidance.

SWIFT

SWIFT supports all efforts to reinforce the security of the global wholesale payments ecosystem, including endpoint security. The escalation in the cyber threat level and the growing sophistication of attackers has been clearly evidenced in recent instances of payment fraud in our customers' local environments. While there is no evidence that SWIFT's network or core messaging services have been compromised in any of these attacks, and while our customers are individually responsible for the security of their own environments, we fully recognise that the security of the industry as a whole is a shared responsibility.

As an industry cooperative, SWIFT is committed to playing an important role in reinforcing and safeguarding the security of the wider ecosystem. In mid-2016 we therefore launched a Customer Security Programme (CSP), a dedicated programme supporting customers to reinforce the security of their SWIFT-related infrastructure.

SWIFT Customer Security Programme

At the outset of the Customer Security Programme we committed to improving information sharing throughout the global community, enhancing SWIFT-related tools for customers and providing control frameworks for customers to self-attest against; we also committed to sharing best practices for fraud detection and enhancing support by third party providers.

Since the CSP launched in May 2016 we have made significant headway. We have introduced enhanced security features to our products to assist SWIFT users in addressing security concerns; these features include stronger default password management, enhanced integrity checking and built-in two-factor authentication (2FA) for those clients using our Alliance Access interface software who did not previously have existing 2FA implementations. We will continue efforts to harden SWIFT-provided products as part of our product roadmaps, and will continue to issue timely security updates to products to allow users to maintain their systems to a high level of protection.

We have also introduced new fraud prevention tools to help customers manage security risk. The tools include our Daily Validation Reports (DVRs) introduced in November 2016 and a Payments Control Service which will launch in 2018. The DVR is a subscription service designed to help institutions strengthen their existing fraud controls by providing a simple and independent means of verifying their messaging activity. The Payment Controls service will enable SWIFT customers to screen their payment messages according to their own chosen parameters, enabling them to immediately detect any unusual message flows *before* transmission.

If organisations suspect they have been targeted or breached, it is vital that they share all relevant information with SWIFT – which is part of their contractual obligations to SWIFT as users of our services.
Our dedicated Customer Security Intelligence team helps limit the community impact by sharing this information in anonymised form, detailing the modus operandi used in the attacks and publishing Indicators of Compromise (IoCs). In mid-2017, SWIFT introduced the SWIFT ISAC global information sharing portal for users to stay aware of our latest technical intelligence – allowing the community to protect itself, take mitigating actions, and defend against further attacks.

In April 2017, SWIFT introduced its Customer Security Controls Framework to drive security improvement and transparency across the global financial community. The Framework comprises a set of baseline security controls – 16 of which are mandatory – that all customers must apply to their SWIFT-related infrastructure. The Framework delivers community transparency by allowing customers to share their self-attestation data with their counterparties and request data from others. This enables customers to incorporate this information into their counterparty risk management and business decision-making processes alongside existing risk considerations such as KYC, sanctions and AML. To prepare customers for this process, we have organised an extensive global campaign, entailing more than 200 work sessions with more than 14,000 attendees in countries all around the world.

In addition, we have also been engaging with vendors and third parties to help secure the wider ecosystem, particularly service bureaux under SWIFT's Shared Infrastructure Programme, and third party interface providers. We have created a directory of cyber security service providers, listing third-parties that can support SWIFT users address cyber security in their organisations and help them comply with the mandatory controls.

On an ongoing basis we continue to urge SWIFT users to prepare by acting in a timely manner on the information and security updates we provide, and ensuring that they meet all mandatory security controls for their SWIFT-related infrastructure; throughout this time, we have been running campaigns to remind customers of the business role, purpose and value of our Relationship Management Application (RMA) which each participant can use to pre-authorise whether or not it is willing to receive messages from other participants, as well as the important role market practice has to play in handling counterparty relationships.

SWIFT strongly believes that the best way to address the security issues faced by the industry is through a community-based approach. For this reason, the Customer Security Programme has been developed – and will continue to evolve – in close collaboration with the SWIFT community and in consultation with our Oversight.

We believe this approach will ensure the Programme evolves in line with the threat and secures a high degree of buy-in from all stakeholders.

Overall Strategy and Seven Elements

We fully support the seven elements outlined by the Committee to help operators and participants to improve security and commend the Committee for undertaking this important survey and considering the promulgation of global guidance in this area. As the Committee will observe, our Customer Security Programme is aligned with the seven elements set out in the discussion note and we greatly appreciate the Committee's efforts to take the Programme into consideration in determining these important principles. We also welcome the fact that the guidance will apply to all end-points, payment systems, and messaging providers, as the adoption of such measures by *all* participants is key to protecting the global financial system.

Development of Guidance

The Committee has correctly observed in its document that any final guidance will require flexibility, allowing both for diversity in approach between operators and participants, as well as for an evolution in these approaches and related risk management tools. We would urge the Committee to ensure that its final guidance does indeed continue to recognise and retain this flexibility.

Moreover, we would respectfully suggest that the Committee include in its guidance a clear recommendation that such flexibility be retained in any transposition of this guidance into domestic rules or regulations.

In this regard, and with respect to the Committee's request for specific input on the points set out under section 6 of the discussion note, we would like to bring particular attention to the first and final points – *Promoting adherence to endpoint security requirements* and *Potentially restricting or suspending a participant's access if and when a participant's endpoint security is determined to be deficient.*

Promoting adherence to endpoint security requirements is vitally important in overcoming the cyber security challenge. Operators, participants – and participants' supervisors all have critical roles to play in this. As mentioned above, SWIFT is committed to playing an important role in reinforcing and safeguarding endpoint security. Through the Customer Security Controls Framework, we not only aim to drive security improvement across the global financial community, but also to enhance transparency around security, thereby promoting participants' adherence to security baselines and enabling participants to better protect against counterparts' cyber risks. Supervisors have an equally important role to play in increasing participants' awareness, incentivising security improvements and in driving adherence. Furthermore, since these endpoint security risks apply to *all* financial institutions, irrespective of whether they are direct participants in a given system or network, supervisors have a vitally important role in ensuring that they too are also included in these efforts.

Regarding *the question of restricting or suspending participants' access*: It is critically important that operators are able to exercise discretion on the suspension or restriction of participants' access to their networks or systems. Imposing prescriptive requirements on operators regarding such suspensions or restrictions would be extremely problematic on several counts. Firstly, codifying the conditions under which operators would have to remove participants (or under which they would *not* be able to remove participants) would increase rather than reduce risk. Secondly, any such prescriptive rules would be based on the false assumption that operators would be aware of any deficiencies in participants' security, and that they would be aware of such deficiencies at all and any given points in time. Thirdly, such rules would risk giving participants a false sense of comfort regarding their counterparts' security. The Committee's final guidance would thus ideally clearly stipulate that discretion in this area must be left to system operators.

The Committee also asks for specific suggestions or evidence of existing good practices and examples of relevant efforts under way that could help advance the strategy and actions that operators, participants and authorities could take to promote adoption of each element. As the Committee correctly observes, every payment system and messaging network has unique attributes; as such, there is no single prescription that can be applied to all systems and networks. This said, we believe that our Customer Security Programme serves as a useful example of an effort that is underway, and we would readily engage with the Committee should it wish to consider any of the elements within our Programme any further.

Information Sharing

Finally, the Committee asks for evidence of any specific challenges related to the seven elements set out in the discussion note. A particular issue we would like to bring to the Committee's attention are the legal barriers related to information sharing. Currently, regulations and laws are unintentionally serving as impediments to efficient information sharing on bad actors, which is hindering effective and targeted cyber risk management.

Financial institutions can help prevent attacks if they know and are able to share information on the so-called "mule accounts" – the end beneficiary accounts to which fraudulent transfers are ultimately directed. Depending on which countries banks are in (and therefore the legal system they abide by) they might not be able to share the information they have on mule accounts either with the banks at which the accounts are held, or with other correspondents, or even, in some cases, with other legal entities within their own groups.

While these requirements are based on sound policy objectives, they can severely limit the timely flow of information and inhibit efforts to prevent cybercrime. There is no question that individuals have the right to privacy and for their personal data to be protected from abuse. However, the goals of safeguarding privacy and detecting and preventing cybercrime are not mutually exclusive. Legal regimes should support and facilitate the fight against cybercrime in ways that pay sufficient regard to individuals' rights to privacy, while also providing a legally certain regime for financial institutions to share cyber fraud related information.

Conclusion

We strongly believe that collaboration is key in the fight against cyber and therefore again thank the Committee for providing the opportunity to provide feedback on this guidance. Again, we look forward to the promulgation of the Committee's final guidance and its adoption across the world. In the meantime, we would like to reassure the Committee of SWIFT's own commitment to continuing to support and complement this work through our Customer Security Programme.

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

Gottfried Leibbrandt
CEO, SWIFT