Dear

Customer Security Programme Newsletter: Q3 2018

Welcome to the third edition of this quarterly newsletter, which is designed to provide you with important information regarding SWIFT's Customer Security Programme (CSP).

The World Economic Forum (WEF) has cited cyberattacks as a top global risk[1] and its analysis shows that, across the globe, the good guys are not winning the fight by any stretch of the imagination – cyberattacks were in the WEF's top ten risks in 2016 and in the top five in 2017; in 2018 they feature in the top three risks to the global economy. It is therefore more important than ever that you continue to secure and protect your SWIFT-related environment, prevent and detect fraud in your commercial relationships, and share and use fraud-related information to defend against future cyber threats.

1. Mandatory security controls:

2018 Attestation: All users need to confirm full compliance with the mandatory security controls V1 (2018) by re-attesting before their current attestation expires on 31 December 2018. Users might wish to use the clarification and guidance included in v2019 to support this work. To facilitate re-attestation, please ensure that your swift.com account and login credentials are up-to-date and extend them, if necessary, before you start your attestation submission.

Controls for 2019: SWIFT has published the new Customer Security Controls Framework (CSCF) v2019, which provides additional guidance on the implementation guidelines and includes changes to the existing controls - these include promoting three controls to a mandatory status and including two new advisory controls. The CSCF v2019 should be consulted, via the User Handbook, to help you plan and budget any action required on your part. The CSCF v2019 will not become effective in the KYC-SA, the online repository for customer attestations until July 2019. Attesting compliance against the CSCF v2019 will be mandatory by the end of 2019. Customers are encouraged to explore the updated suite of SWIFTSmart training modules reflecting the different changes.

Change Management: The Change Management process to evolve the controls framework is designed to ensure that the SWIFT community has sufficient time (up to 18 months) to understand and implement any future changes to the controls requirements. Any changes to the controls will be announced mid-year, with attestation and compliance against the mandatory controls of any new version required between July and December of the following year, dependent on the expiry date of the attestation. In exceptional circumstances an emergency release may be required, but we expect this to be a rare occurrence.

KYC-SA enhancements: A number of enhancements have been made to the KYC Security Attestation (KYC-SA) application that will improve the user-friendliness of the application and help to address a number of challenges faced by the community, as follows:

- Users now have a view in the KYC-SA of all the counterparties they have exchanged SWIFT traffic with over the past year, making it easier to identify which counterparties they need to access in the KYC-SA.

[1] The Global Risks Report, published by the World Economic Forum on 17 January, 2018.

- Users are able to bulk process access requests or 'whitelist' counterparties upfront rather than handling numerous access requests one-by-one.
- Users can extract KYC-SA data securely for inclusion of their assessment in their risk management processes and to strengthen security even more, we have introduced the KYC-SA role of 'security officer' to generate these sensitive business reports.

These new features are available now and further details of these and other enhancements can be found in the KYC-SA Release Letter dated 22 June 2018, which is included in the User Handbook.

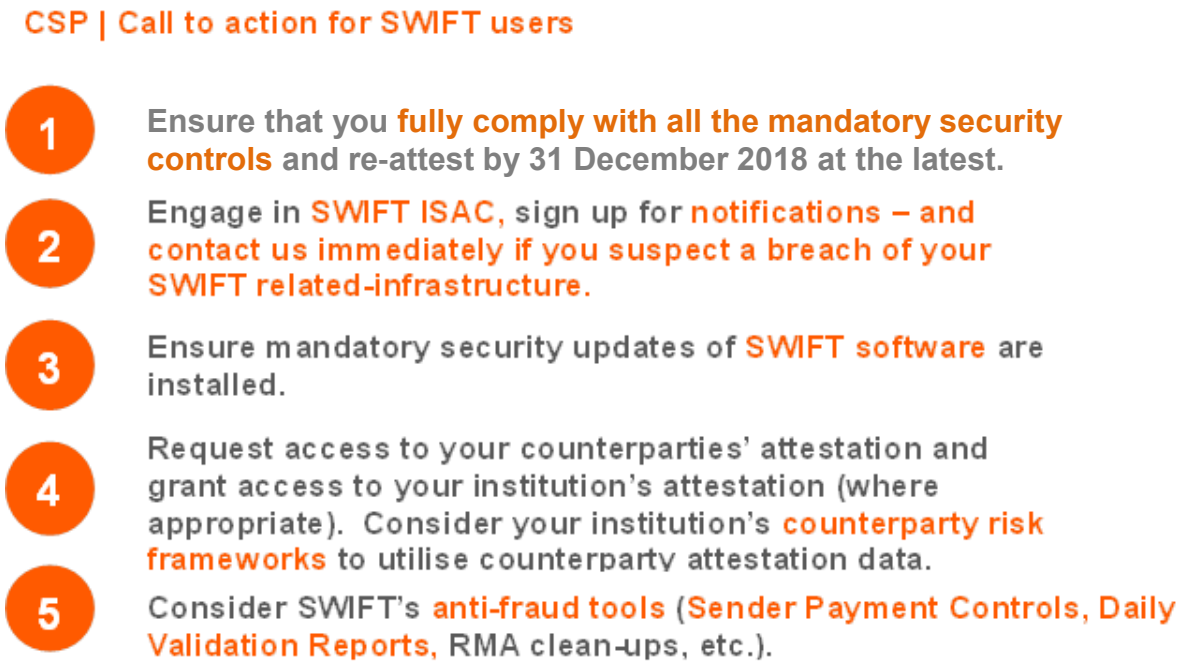
2. **SWIFT ISAC:** If you have not yet subscribed to the SWIFT ISAC, we encourage you to do so. This will give you access to details on indicators of compromise (IOC), information about malware samples observed, and descriptions, where possible, of the modus operandi used by attackers. You can also subscribe to the Security Notifications to ensure you receive immediate alerts when something new is published. Access to the SWIFT ISAC is available via swift.com, using your existing swift.com login credentials. We also suggest that, as a precaution, you familiarise yourself with the Cyber Security Incident Recovery Roadmap, which is set out in bulletin 10047 in the SWIFT ISAC.

3. **SWIFT software:** Under the Customer Security Controls Framework, the mandatory control 2.2 on security updates requires that mandatory software updates are applied by the relevant deadlines. We remind you that the Alliance and SWIFTNet Release 7.2 is mandatory and must be implemented by the end of November 2018 at the latest.

4. **Counterparty Risk Frameworks:** SWIFT strongly recommends that you request access to your counterparties' attestation details and give them permission to view yours, where appropriate. This will create an opportunity for organisations to be transparent about their attestation status, which should increase the trust and confidence for counterparts doing business with each other. To ensure that access requests are handled without delay, you should assign the "Granter" and "Requester" roles in the KYC-SA if these roles are still outstanding. As best practice, you should accept or reject access requests as quickly as possible and within a maximum of six business days. While you are defining the process for approving and granting access, you can reject requests in the meantime and ask your counterparty to request access again in the future.

5. **Anti-fraud tools:** Our new fraud prevention service, SWIFT Payment Controls, is due to be launched later this year. Designed to protect your payment operations against fraudulent attacks, this anti-fraud solution helps strengthen your security strategy. SWIFT Payment Controls combines real-time monitoring, alerting and blocking of sent payments, with daily reporting. It helps institutions detect and prevent high risk payments and mitigates business disruption and financial losses in the event of back-office compromise.

Where to get help: Please consult the security attestation support page, accessible via mySWIFT, for information that will help you complete your security attestation, and for access to a range of useful links. If you require further support you can also consult the CSP materials available via the User Handbook, the SWIFTSmart training portfolio, Knowledge Based Tips, videos, webinar recordings, and FAQs. For guidance and information, some documents and SWIFTSmart training modules are available in a range of languages, and we regularly host webinars and information sessions in local languages. For further information, please contact your SWIFT account manager.



You have received this newsletter because you have been identified as a point of contact for CSP or because you are a registered user in the KYC-SA application as part of the attestation process for your organisation. If relevant, please forward this newsletter to colleagues within your organisation.

Yours sincerely,