Dear

Customer Security Programme Newsletter: Q2 2018

Welcome to the second edition of this quarterly newsletter, which aims to keep you informed of important information regarding SWIFT's Customer Security Programme (CSP).

In April 2018, the Association for Financial Professionals (AFP) published its "Payments Fraud and Control Survey" report, stating that 78% of the organisations surveyed had experienced payments fraud in the previous year. Clearly the cyber threat is here to stay and it is essential, therefore, that you implement preventive measures to protect your SWIFT infrastructure, as outlined in the five key steps below:

CSP | Call to action for SWIFT users

1. **Engage in SWIFT ISAC, sign up for notifications – and contact us immediately if you suspect a breach of your SWIFT related-infrastructure.**
2. **Ensure mandatory security updates of SWIFT software are installed.**
3. **Ensure that you fully comply with all the mandatory security controls and re-attest by 31 December 2018.**
4. **Request access to your counterparties' attestation and grant access to your institution's attestation (where appropriate). Consider your institution's counterparty risk frameworks to utilise counterparty attestation data.**
5. **Consider SWIFT's anti-fraud tools (Sender Payment Controls, Daily Validation Reports, RMA clean-ups, etc.).**

SWIFT ISAC: There is a wealth information contained in the SWIFT ISAC, such as details on indicators of compromise (IOC), information about malware samples observed, and descriptions (when possible) of the modus operandi used by attackers. The SWIFT ISAC now allows the automated exchange of information relating to cyber threats, using industry standard formats (STIX/TAXII). If you are interested in subscribing to the automated flow, please refer to the SWIFT ISAC in bulletin 10073, which can be found at swift.com>isac>report>10073

SWIFT software: The Alliance and SWIFTNet Release 7.2, which provides a number of security enhancements and related features, is mandatory and must be implemented no later than November 2018. As part of the upgrade to Release 7.2 you must install the latest software updates, including the latest fixes. Release 7.3 will be available from end of August 2018, a pre-requisite of which is the implementation of the mandatory 7.2 release. This annual release will provide security features in support of the CSP programme, including additional options to implement multi-factor authentication (MFA) on your Alliance GUIs. You will find more information on the 7.3 release in the April operational and premium newsletters.

Mandatory security controls: The priority for 2018 is to confirm your compliance with all the mandatory security controls and close any gaps you may have identified in your initial assessment of compliance with the mandatory controls. There are no changes to the current Customer Security Controls Framework v1 (v2018), against which you must re-attest before the expiration of the one-year validity period of your current attestation. Further assistance is available at swift.com>myswift>customer-security-programme-csp.

Counterparty Risk Frameworks: You should now be requesting access to your counterparties' attestation details and giving them permission to view yours, where appropriate. To help you, we have created a video that explains how to grant access to other institutions to view your data in the KYC-SA application, and how to request access to view theirs. The video is available at swift.com>kb>resources>5021828.document>04_kyc_sa_dataconsumption.mp4. You can start your online evaluation of your counterparties' self-attestation data in the KYC-SA application and to record the high-level outcome of such evaluations against your cyber risk management framework and policies business decision-making processes, along with other risk considerations such as KYC, sanctions and AML.

Anti-fraud tools: There are additional measures you can take that will provide further protection against cyber threats. Anti-fraud tools can help customers by analysing data and looking for trends and anomalies that can help to pre-empt potential attacks. SWIFT's Daily Validation Reports provide a global summary of your inbound and outbound counterparty payment flows, based on SWIFT's own records of your transaction activity. They support validation and easy reconciliation against your system records. If suspicious or fraudulent activity occurs, they provide SWIFT information you need to help you cancel messages and recover funds, protecting you, your customers, and your counterparties. SWIFT's Relationship Management Application (RMA) plays an important part in supporting trusted communication between different users. We encourage users to regularly review and clean up RMA relationships and to consider the adoption of RMA Plus, which allows users to control which message types they accept to receive from and send to their counterparties.

Future developments: Watch this space for news on developments to aspects of the CSP. Over the coming months we will update you on the Customer Security Controls Framework v2 (v2019) and the process for controls changes; enhancements to the KYC Security Attestation application; and the introduction in Q3 2018 of our Sender Payment Controls service, which will bring additional safeguards to ensure that payment instructions are in line with business expectations.

Save the date: You will be able to engage with members of our CISO team and/or our regional Customer Security Programme experts at our forthcoming business forums, as follows:

24 April: London Business Forum, London
08 May: India and subcontinents Regional Conference, Mumbai
08-09 May: Benelux Business Forum, Brussels
05 June: Greater China Regional Conference, Shanghai
18-20 June: Russia Business Forum, Moscow

SWIFT will also participate at the FS-ISAC Summit, in Boca Raton, which takes place from 20-23 May.

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,