Dear

Customer Security Programme Newsletter – Q1 2018

Welcome to the first edition of this quarterly newsletter, which aims to keep you informed of important information regarding SWIFT's Customer Security Programme (CSP). You have received this newsletter because you have been identified as a point of contact for CSP or are a registered user in the KYC-SA and part of the attestation process for your organisation.

Attestation on your Level of Compliance

We are very encouraged by the excellent response to the CSP – it is testament to how seriously the SWIFT community is taking the cyber-security threat. We are pleased to report that 89% of the connected and live BIC8s on the SWIFT network submitted their attestations by the December 31st deadline, and this percentage continues to rise as several hundred organisations have attested since or have attestations in progress. Combined, these institutions account for over 99% of all FIN messages sent over the SWIFT network.

If you have not yet attested, you should do so as soon as possible. You will find detailed information and resources on how to attest on the CSP webpages on swift.com – from there you can also log into the KYC-SA tool to complete your submission. Customers are reminded that SWIFT reserves the right to inform financial supervisors of SWIFT users that have not yet attested.

Compliance with the Security Controls

The priority for 2018 is to confirm full compliance with the mandatory security controls. Any gaps you identified when you assessed your compliance with the mandatory controls will need to be closed, and you should re-attest to your compliance with all mandatory controls by year-end. If you require additional support please refer to the CSP materials available via the User Handbook, SWIFTSmart training portfolio, mySWIFT, Knowledge Based Tips, Videos, Webinar recordings, and FAQs.

SWIFT has published a directory of cyber security service providers that could assist you in this process. Should you engage an independent internal or external expert to support your assessment and attestation process, you will need to indicate this in the "Assessment Type" field in the KYC-SA. In December, we introduced advisory assessment types, which allow you to highlight if you have had an Independent Advisory Review executed by an Internal team or External provider.

Interface Readiness

In 2017 your interface vendors also met the challenge to raise the bar on cyber resilience embedded or supported in their products. The Certified Interface Programme is designed to ensure that SWIFT interfaces developed by third-parties meet stringent conformance and security requirements, including a set mandatory and advisory security requirements which have been adapted from the Customer Security Controls Framework. Interface providers were requested to self-attest their compliance against the security controls by the end of December 2017 to qualify for interim certification and to be listed on the certification registry on swift.com. For an interface provider to qualify for full certification, a customer of their choice has to verify and confirm the interface provider's self-attestation. Interface providers must receive customer confirmation by mid-2018 to obtain full certification. We recommend that customers check the status of their messaging interface provider's certification on swift.com.

SWIFT's Alliance and SWIFTNet Release 7.2, which was made available in August 2017, provided a number of security enhancements and related features. In November 2017, we delivered the quarterly security update for our messaging and connectivity interface products. We will continue to provide security updates for SWIFTNet and Alliance products on a quarterly basis in 2018. We have finalised the products security roadmap for the 7.3 release and will be communicating on release content through existing channels towards the end of Q1 2018.

Consumption and Risk Management

In addition to addressing any compliance gaps, you should also be requesting access to your counterparties' attestation and giving them permission to view your attestation details. This allows you to start assessing your counterparty attestation data against your cyber risk management framework and policies, alongside other risk considerations such as KYC, sanctions and AML. Using the KYC-SA, you can share attestation data with your counterparties and request data from others. You are in control of your attestation data – you can grant or deny requests to view your attestation data.

Prevention and Detection

Daily Validation Reports, launched in 2016, is a fraud detection tool that allows customers to verify SWIFT message flows and detect unusual transaction patterns and new and uncharacteristic payment relationships. The reports have been well received by the community. Following the success of Daily Validation Reports, and based on requests from corporates, a new release at the end of Q1 2018 will also allow user to access details of their MT101 messages.

Our Payment Controls service, to be launched in Q3 2018, is an 'in-flight' service that monitors payment messages in real-time in the SWIFT network. It will bring additional safeguards to ensure that payment instructions are in line with business expectations and don't represent a significant or unacceptable business risk. Initially targeted at smaller financial institutions or subsidiaries of larger institutions, the Payment Controls service will be launched as a hosted utility solution, which will allow SWIFT users to access it instantly, with no hardware or software installation or maintenance.

SWIFT's Relationship Management Application (RMA) plays an important part in supporting communication between different financial institutions. Against the backdrop of the current cyber-threats, we continue to encourage institutions to review and clean-up RMA relationships and to consider the adoption of RMA Plus.

Further information on the Daily Validation Reports, Payment Controls, and RMA can be found on swift.com.

Information Sharing

The cyber-threat against our industry is very persistent, adaptive and sophisticated – and it is here to stay. In December 2017, SWIFT and cyber security specialists, BAE Systems, produced a report based on the evolving cyber threat, which is based on evidence gained from detailed forensic examinations of a range of recent cyber-attacks on SWIFT customers. The report evidences the value of threat information sharing, and showcases how the resulting findings can be used to help protect against the cyber threat. The report is available to customers in the SWIFT ISAC.

Information-sharing is very important in helping customers to better defend themselves against potential future cyber-attacks, and SWIFT provides a lot of support in helping customers keep up with the threat. In May 2017, SWIFT introduced the SWIFT ISAC global information sharing portal to share intelligence, which allows the community to protect itself, take mitigating actions, and defend against further attacks. This information includes indicators of compromise such as file hashes and details about malware samples observed. When possible, Modus Operandi used by attackers is described and machine-digestible files are provided (YARA rules, OpenIOC, etc.). In February 2018, a new release of the SWIFT ISAC will be issued to allow the automated exchange of cyber-threat information using industry standard formats (STIX/TAXII).

Quality Assurance

SWIFT's Customer Security Controls Framework and Attestation Process are designed to drive cyber security improvements and transparency across the global financial community. Implementing a quality assurance framework is one of the measures that will be put in place to assure the ongoing quality and effectiveness of the overall framework. This may involve requiring users to provide follow-up information to further substantiate their attestations or, more generally, to evaluate and identify possible adjustments to the overall framework. Further details will be shared with the community by the end of Q1.

Other measures to assure the quality of the attestation process include developing analytics based on anonymised and aggregated data from the KYC-SA platform and SWIFT's customer-facing activities (such as the Support Helpdesk), and general surveys and interviews to gather feedback across all user segments.

Changes to the Controls Framework and Re-Attestation

There are no planned changes to the controls requirements that are effective in 2018, as per the current version of the Customer Security Controls Framework (v1, published April 2017).

The Customer Security Controls Framework is built upon the principle of self-attestation and the transparent exchange of information. To encourage community transparency, SWIFT is preparing to communicate to supervisors, the users within their jurisdiction that have not submitted a valid attestation, and as of 1 January 2019, SWIFT reserves the right to notify local supervisors of users that have failed to timely re-attest or have not confirmed full compliance with the mandatory controls. In the case of users that are not supervised, SWIFT plans to make a report available to messaging counterparties to look up those users that have not attested, and as of 2019 users that are not compliant.

Save the date

6 March 2018, Dubai: we will be discussing the cyber threat at a roundtable event involving Chief Information Security Officers from major banks across the region.

Yours sincerely,