Customer Security Programme Newsletter: Q4 2018

Welcome to the fourth edition of our quarterly newsletter – designed to provide you with the important information you need to know about SWIFT's Customer Security Programme (CSP).

During a recent Sibos debate on cyber security, each of the three highly-respected panellists were asked if a 'cyber 9/11' event – one that completely 'redraws the battle lines' – would happen in the next ten years. They all agreed that it probably would – with one stating that ten years was perhaps "too wide a range".

With such a menacing vista, it is more important than ever that you continue to protect and secure 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.

This newsletter will share the latest news and updates from the SWIFT Customer Security Programme team to help you defend your business.

Payment Controls Service – available now

Our new intelligent in-network solution to combat fraudulent payments, the Payment Controls Service, is now live and available to add to your organisation's fraud defences. This new service helps payment operations teams reduce fraud risk in real-time through its unique alerting and reporting capabilities – and may be set to flag, hold, release or reject high-risk or uncharacteristic payments, according to business needs. The service is hosted in the SWIFT cloud to allow users immediate access, with no hardware or software installation or maintenance. For more details about the Payment Controls Service, please see here.

SELF-ATTEST COMPLIANCE AGAINST MANDATORY CONTROLS BY 31 DECEMBER

The re-attestation deadline is only a few weeks away. All SWIFT users *must* self-attest compliance with the mandatory controls set out in SWIFT's Customer Security Controls Framework (v1) by 31 December.

The KYC Registry Security Attestation (KYC-SA) application is the tool for users to self-attest – and every day we are seeing more and more SWIFT users publish their attestations. If you have not done so yet, please follow the necessary steps and submit your self-attestation before the deadline.

New features

This self-attestation data is critical for the community as it will help SWIFT users determine if they are comfortable doing business with different counterparties from a cyber risk management perspective. The KYC-SA tool allows users to bilaterally share attestation information with counterparties.

Two significant improvements have been made to the KYC-SA tool since the last newsletter and both dramatically improve the user-friendliness of the application and make the process faster and easier:

Bulk Access Request. This function means you can now send access requests to multiple counterparties in one go instead of sending individual requests. This will prove particularly useful when you have a long list of counterparties identified that you want to request access to.

Auto-grant. This function means you can now store up a list of counterparties that would automatically be granted access to your data upon receipt of an access request – thus saving you having to go through each request one-by-one. This ensures a speedy response time to pre-approved access requests and means you can focus on access requests sent by other counterparties.

Independent assessments

To safeguard and improve the quality and effectiveness of the Customer Security Control Framework and the associated self-attestation process across its user community, SWIFT reserves the right to request additional independent assurance to further substantiate users' self-attestations. Having evaluated customers' attestations across a series of factors as part of a quality assurance process, we have begun requesting a select number of customers to arrange for independent external assessments to verify the veracity of their attestation.

These assessments will need to be performed by independent specialists that possess the necessary technical capabilities to undertake the work. If the assessments highlight that the customer's current implementation does not match that attestation recorded in KYC-SA, then a new attestation will need to be made.

Two new reports – BAE Systems and ISSA

SWIFT has co-authored two cyber security white papers, which were both published at Sibos:

- 'The Evolving Advanced Cyber Threat to Financial Markets' with BAE Systems – which looks at potential vulnerabilities from 'Advance Persistent Threat' attacks across banking, securities, foreign exchange and trade finance markets.
- 'Cyber Security Risks in Securities Market' with ISSA (the International Securities Services Association) – which looks at potential vulnerabilities within the securities servicing and custody flows.

Useful information

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.

If you have any questions, please contact your SWIFT account manager.

Thank you

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

Please feel free to forward this newsletter to colleagues within your organisation.