Customer Security Programme Updates

Reinforcing the security of the global banking system

July 2019

Welcome to the SWIFT Customer Security Programme (CSP) quarterly update – designed to provide you with the latest important information and updates relating to the CSP.

2019 KYC-SA window now open

The KYC Security Attestation (KYC-SA) application for the Customer Security Controls Framework (CSCF) v2019 is now available and customers can start to attest their level of compliance against this new baseline. The CSCF v2019 was published last year and is available here (SWIFT login ID required).

The KYC-SA is an online repository for customer self-attestations that allows institutions to report their levels of compliance with the requirements outlined in the Customer Security Controls Policy (SWIFT login ID required). No additional software or hardware is required to access the browser-based application, which uses a secure two-step verification process.

Once your self-attestation data has been prepared and submitted, SWIFT will publish your submission securely, which can then be consulted by other customers and used in their

counterparty risk management processes. The presence of the self-attestation and its validity will be visible to all KYC-SA users, but the data contents will not be shared without the owner's explicit permission.

The re-attestation on the CSCF v2019 deadline is **31 December 2019** and all SWIFT users must self-attest compliance with the mandatory controls set out in SWIFT's CSCF by this date.

Independent Assessment Framework

At the request of the community and following the Board's and Overseers' approval, SWIFT has published a new Independent Assessment Framework (IAF) to support its users and their independent assessors in carrying out their responsibilities as part of the CSP. The Framework is available to SWIFT users here (SWIFT login ID required).

From July 2020, all SWIFT users will be obligated to carry out an independent assessment when self-attesting. These can be done through either:

- **Internal assessment** carried out by your company's second- or third- line of defence such as internal compliance, internal risk or internal audit departments (independent from the first line of defence function submitting the attestation); or
- **external assessment** carried out by an independent external organisation with cyber security assessment experience and individual assessors who have relevant security industry certification.

Independent assessments must cover, at the minimum, all mandatory controls as set out in the latest CSCF version, which are applicable to that user based on its CSP architecture type and infrastructure. Users that have attested against the advisory controls may also wish to consider requesting that the assessor also include these in their review.

For 2020, we encourage users to plan and budget any actions that might be required on their end to achieve, on time, such

that might be required on their end to achieve, on time, such independent assessment. In addition to the independent assessment framework outlined above, SWIFT continues to reserve the right, for a small cross-section of users, to mandate that an **external** assessment be undertaken.

Coming soon

In the coming weeks SWIFT will formally announce the availability of the forthcoming CSCF version (v2020). You can already access the CSCF 2020 here (SWIFT login ID required). In addition, an updated version of the Customer Security Control Policy governing the CSP Programme will be published soon.

Alliance suite Release 7.4

The mandatory upgrade to R7.4 of SWIFT's Alliance interface products will be available from August. This release applies to Alliance Access, Alliance Entry, Alliance Gateway, Alliance Web Platform Server-Embedded and SWIFTNet Link and SWIFT Web Access.

It will be necessary for customers to remotely upgrade their products to ensure that their SWIFT services remain uninterrupted. The aim of the release is to continue to provide a highly secure and efficient SWIFT service for our customers in the years ahead.

New report – Three Years on from Bangladesh

In April, we published a new cyber report, *'Three years on from Bangladesh: tackling the adversaries'*, providing new insights into the evolving nature of the cyber threats facing the global financial community.

Key findings show that:

- Four out of every five of all fraudulent transactions were issued to Beneficiary accounts in East and South East Asia
- Approximately 70 per cent of attempted thefts were USD-based – but usage of European currencies increased
- The value of each individual attempted fraudulent transaction decreased dramatically – from more than USD$10m to between USD$250,000 and USD$2m

Based on investigations conducted over the last 15 months, the report shows how closer industry collaboration resulted in the quick identification of financial institutions targeted by cyber criminals – in most cases, before attackers were even able to generate fraudulent messages.

Read more >

'Getting Started Guide' in local languages

SWIFT recently published a new guide to assist financial institutions in assessing levels of cybersecurity risk in their counterparties and incorporate it into their risk management frameworks.

Assessing Cybersecurity Counterparty Risk - A Getting Started Guide, provides a series of practical, but non-binding set of information and recommendations, including how to establish a governance model, create a cybersecurity risk management framework and how to adopt cybersecurity risk countermeasures.

Versions of the *Getting Started Guide* are now available on the SWIFT website in French, German, Spanish, Russian, Japanese, Korean, and Chinese – both traditional and simplified.

Getting Started Guide

Gottfried Leibbrandt at G7 Cyber Security Conference in Paris

The outgoing SWIFT CEO Gottfried Leibbrandt joined the G7 Cyber Security Conference in Paris in May for a high-level gathering to discuss the rising cyber security challenge. Under the French G7 Presidency, the Governor of the Banque de France and the Minister for the Economy and Finance welcomed an eminent delegation of public and private sector speakers and experts under the theme, *Coordinating efforts to protect the financial sector in the global economy*.

Leibbrandt joined a panel titled, Challenges for the financial sector in adapting to cyber threats, alongside respected authorities, including the Banca d'Italia, the German Finance Ministry, as well as DTCC and Euroclear.

In his remarks, the last major public intervention before his departure, Leibbrandt focussed on the challenges for supervisors and regulators, emphasising that given the international nature of the threat, the response too has to be international.

New articles published

As we know, fraud remains a top global threat to the financial sector – and is evolving on a daily basis. The sophistication of threat actors is increasing and virtually any organisation can be a target. Recently, we published a series of three articles looking at:

Five ways you could fall prey to payments fraud ›

The anatomy of a cyberattack ›

Fighting fraud – can you keep up? ›

And finally...

With only three months to go until Sibos 2019 in London, we are

putting together another rich conference programme that is now available. Please visit www.sibos.com for more details and to register to attend.

Stay connected

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way. As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.