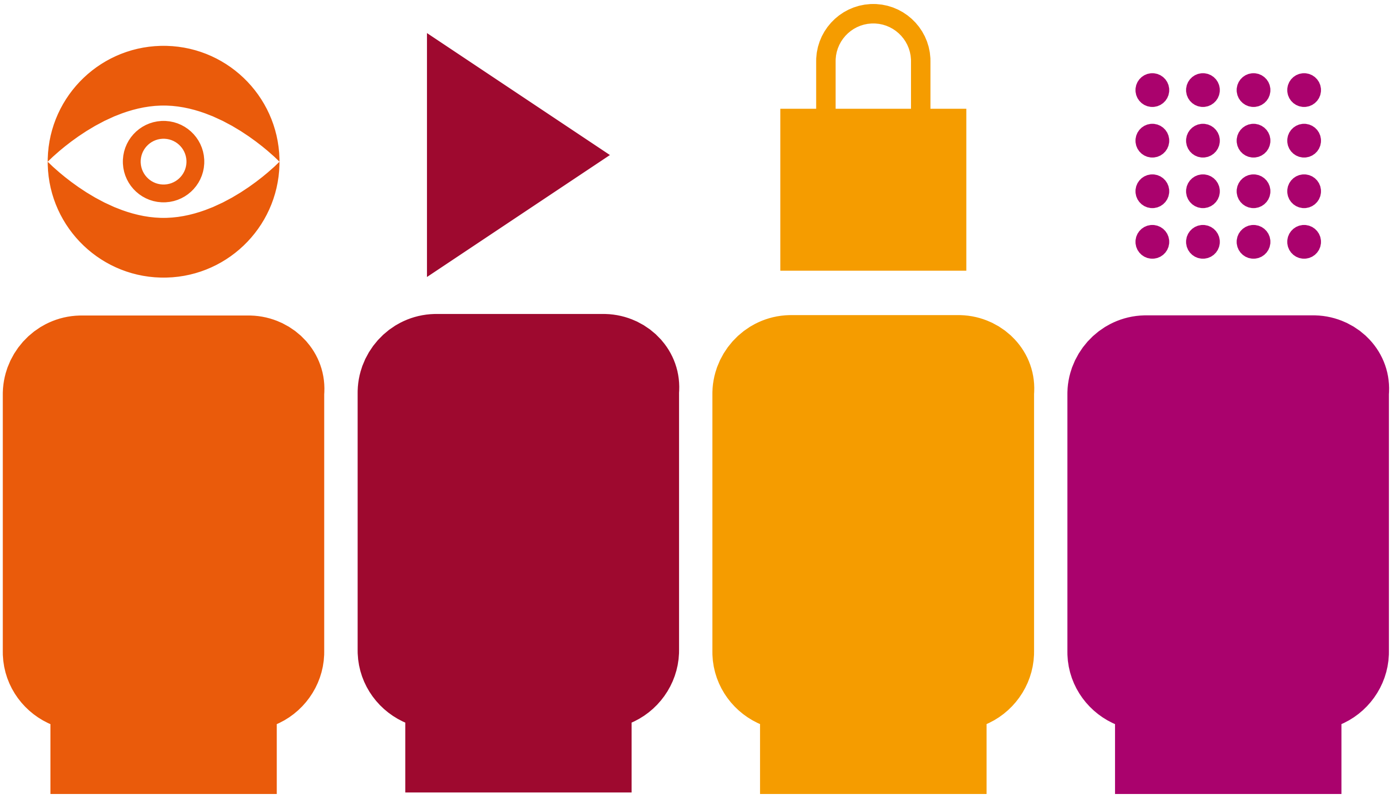
SWIFT
Customer Security Programme

Reinforcing the security of the global financial community



Cyber is the second most reported economic crime affecting organisations

In 2016, SWIFT introduced its Customer Security Programme (CSP) – a dedicated programme to support customers in reinforcing the security of their SWIFT-related infrastructure.

The CSP addresses three key aspects: the security and protection of customers' local environments, preventing and detecting fraud in their counterparty relationships, and working together as a community to prevent future cyber-attacks.

The programme includes the introduction of mandatory customer security controls, new services to help customers prevent and detect fraudulent activity, and community-wide information sharing initiatives to strengthen defences through the exchange of intelligence information.

As a global cooperative, SWIFT is committed to playing a significant role in support of its customers and community.

> **“While each individual SWIFT customer is responsible for the security of its own environment, the security of the global community can only be ensured collectively. It requires a collaborative approach between SWIFT, its customers, overseers and third party suppliers. SWIFT is fully committed to leading the community effort required to keep global banking safe, and deploying its knowledge and expertise to help customers in the fight against the persistent threat of cyber-attacks.**
>
> **Gottfried Leibbrandt**
> **CEO, SWIFT**

40%

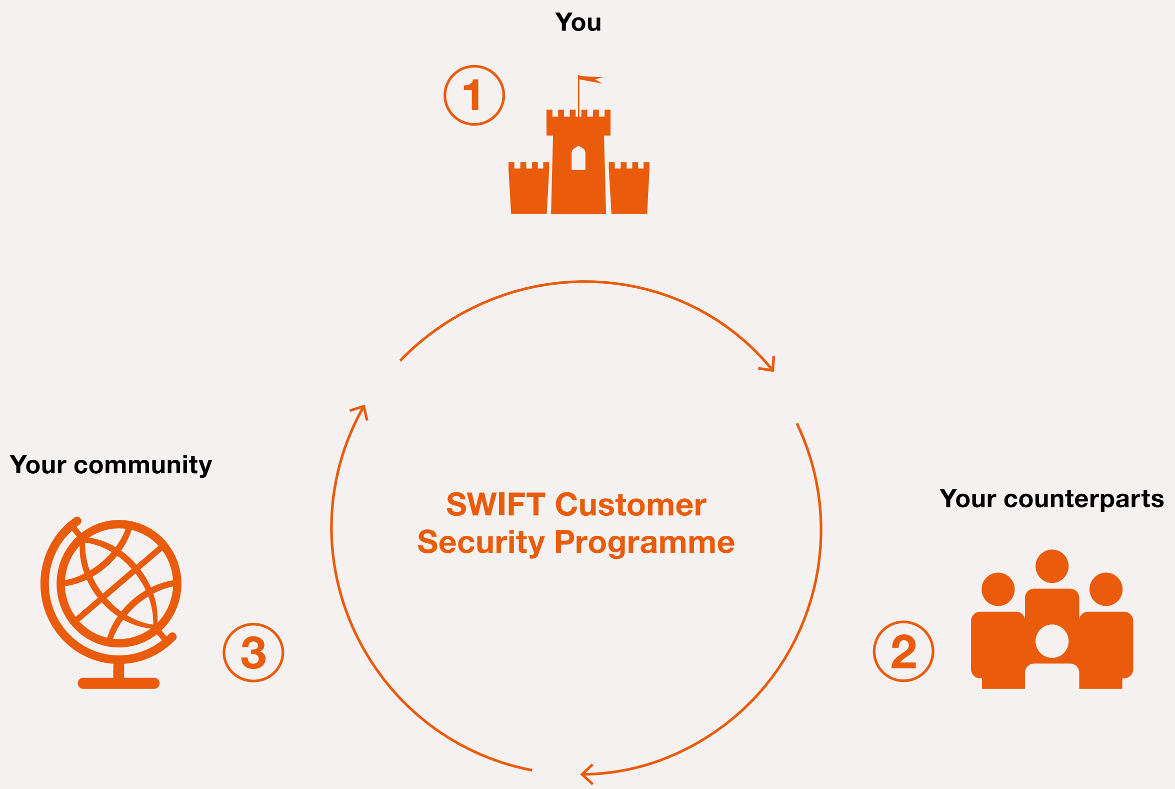
increase in cyber-attacks targeting financial institutions in 2016

41%

of financial institutions consider cyber as one of the top three risks affecting their institution over the next two years

CSP Objectives

The CSP is articulated around three mutually reinforcing areas.



You

1

Your counterparts

2

Your community

3

SWIFT Customer Security Programme

Contact us if you have any cyber concerns
The sooner you contact us, the more likely we may be able to help to minimise the community-wide impact of an attack. If you have concerns, you can contact our customer support teams worldwide, 24/7. **www.swift.com/contact-us/support**

Sign-up for the SWIFT ISAC portal
SWIFT provides anonymised information on known attacks, including indicators of compromise and modus operandi. We make this available to all users via the SWIFT 'Information Sharing and Analysis Center' (ISAC) global portal. **www2.swift.com/isac**

Check out our new Payment Controls offer
Set for launch in 2018, this service monitors your in-flight transactions for out-of-policy and suspicious payments, proactively defending your business against fraud. **www.swift.com/paymentcontrols**

Learn more about the CSP
Find out the latest news, updates and documentation on the CSP. **www.swift.com/csp**

1

You
Secure and protect

You first need to secure and protect your local environment

A fundamental message of the CSP is for your organisation to secure its own local environment, including the physical set-up of your local SWIFT-related infrastructure. It is also about putting in place the right policies and practices to avoid cyber-related fraud. Breaches in local infrastructure have been a common starting point for known cyber-attacks.

2

Your counterparts
Prevent and detect

You also need to prevent and detect fraud in your commercial relationships

Even with strong security measures in place, attackers are very sophisticated and it is vital to manage security risks in your counterparty relationships so that you can minimise the risk associated with payment flows. Strong prevention and detection measures are necessary alongside the foundations of good security practices in your organisation.

3

Your community
Share and prepare

Finally, you should continuously share information and prepare against future cyber-threats in collaboration with others

The financial industry is global, and so are the cyber challenges it faces. Attackers can rapidly scale and replicate fraud worldwide, so constant vigilance is of the highest importance. We remind all customers that it is vital to share all relevant information and to inform SWIFT if there is a problem linked to your SWIFT-related infrastructure – this is a contractual obligation for all SWIFT users.

To create a security baseline for the global financial community, SWIFT has introduced a set of core security controls that all users must meet to secure their local SWIFT-related infrastructure.

Detailed security controls (16 mandatory and 11 advisory) have been published, and documentation is available in the CSP section of the User Handbook on swift.com. All controls have been defined by SWIFT and industry experts and are articulated around three overarching objectives and eight principles:

SWIFT Customer Security Controls Framework

Secure your environment
1 Restrict internet access
2 Segregate critical systems from general IT environment
3 Reduce attack surface and vulnerabilities
4 Physically secure the environment

Know and limit access
5 Prevent compromise of credentials
6 Manage identities and segregate privileges

Detect and respond
7 Detect anomalous activity to system or transaction records
8 Plan for incident response and information sharing

The control definitions are in line with existing information security industry standards, and are product-agnostic.

16 mandatory and 11 advisory cyber security controls

Know the cyber security controls.

Know cyber.

Below are some key questions and answers to explain the process in more detail.

What is the purpose of the customer security attestation process?
Through the attestation process, SWIFT is increasing the overall level of transparency on cyber security among users of the SWIFT network.

What practical steps should our organisation take to comply with the mandatory security controls?
Please read and take time to understand the SWIFT Customer Security Controls Framework and the Customer Security Controls Policy that outlines the related attestation process.

You can 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.

SWIFTSmart training modules related to the Framework are also available on swift.com.

www.swift.com/myswift/customer-security-programme-csp

How can we find third parties to help us implement the controls?
You can call upon third parties to help you to implement the Customer Security Controls.

SWIFT has published a directory of cyber security service providers on swift.com to help you to identify possible project partners.

www.swift.com/myswift/customer-security-programme-csp_/community-engagement/cyber-firms-directory

How do we attest?
SWIFT has opened the KYC Registry Security Attestation Application (KYC-SA) as the place to submit your attestation information. All SWIFT users can submit their attestation data in this application. You do not need to be a current user of the KYC Registry.

All SWIFT users received a Welcome Mail in July 2017 (sent to swift.com administrators of the parent entities) which provides your KYC-SA login details and sets out the practical steps to complete the attestation.

www.swift.com/the-kyc-registry-security-attestation-application

What happens when your attestation data has reached the KYC-SA?
The data remains yours and it is stored securely. Your counterparts are able to send you a request to view your attestation data. This creates an opportunity for your organisation to be transparent about your attestation status, which may increase the trust and confidence of your counterparts in doing business with you.

You have full discretion and may choose to grant or reject access to such requests.

We completed our attestation in 2017, what next?
You will need to re-attest and confirm full compliance with the mandatory security controls by the end of 2018.

Attestations will also have to be renewed annually thereafter.

If required, you will need to undergo any necessary project work to ensure your operations are fully compliant with the controls.

What about viewing the compliance status of my own counterparts?
Customers should begin to incorporate their counterparties' attestation data into their risk management and business decision-making processes – alongside other risk considerations such as KYC, sanctions and AML.

Using the KYC-SA, customers can share their attestation data with their counterparties and request data from others. This creates an opportunity for an organisation to be transparent about their attestation status, which should increase the trust and confidence for counterparts doing business with each other.

This is not a 'one-off' exercise: SWIFT's Customer Security Controls Framework will evolve over time in light of the changing cyber-threat landscape.

Organisations should view self-attestation as part of an ongoing cycle of change management to drive real-world improvements in security.

Follow-up actions by SWIFT

To support the effectiveness of the Customer Security Controls Framework, SWIFT reserves the right to report to supervisors or others, as applicable, the names of users that fail to complete their self attestation or fail to comply with all mandatory security controls by the relevant deadlines. Reporting to supervisors starts in 2018, and will continue on an annual basis.

- From January 2018, SWIFT reserves the right to report users that have failed to submit a self-attestation.
- From January 2019, SWIFT reserves the right to report users who have failed to comply with all mandatory security controls (or who connect through a non-compliant service provider).
- For users that are not supervised, identical circumstances and data may be reported by SWIFT to their messaging counterparts.

SWIFT tools

To help customers meet our security requirements, SWIFT has introduced new security features to its software – such as the mandatory use of two-factor authentication (2FA) – and we will and we will continue to do so as part of our product roadmaps. We also continue to issue regular security updates to SWIFT products and plan to do so on a quarterly basis.

SWIFT has made security guidance documents for each of our interfaces available in the Knowledge Base on swift.com. This includes expanded guidance published for Alliance Access and Entry, for Alliance Lite2 and for qualified third-party interfaces.

The aim of this upgrade is to continue to provide a highly secure and efficient SWIFT service for our customers in the future. It will apply to Alliance Access, Alliance Entry, Alliance Gateway, Alliance Web Platform Server-Embedded and SWIFTNet Link products.

www.swift.com/our-solutions/a-to-z/release-7_2

Staying up to date with the latest software is essential.

Know cyber.

31 December

2017

The initial deadline for all SWIFT users to have self-attested their level of compliance with the mandatory security controls.

1 January

2018

From January 2018, SWIFT reserves the right to report users that have failed to submit a self-attestation.

31 December

2018

The deadline for all users to re-attest and to confirm full compliance with the mandatory security controls.

1 January

2019

From January 2019, SWIFT reserves the right to report users who have failed to comply with all mandatory security controls (or who connect through a non-compliant service provider), over the next two years.

SWIFT has put in place a number of self-service tools and materials such as the SWIFT Customer Security Controls Framework and Customer Security Controls Policy documents, FAQs, SWIFTSmart training modules and other swift.com resources such as MySWIFT.

Know cyber.

Through the attestation process, SWIFT is increasing the overall level of transparency on cyber security among many users of the SWIFT network.

Planning

Understanding the controls
Get to know the 16 mandatory and 11 advisory security controls

Conducting a gap analysis
Find out your security status in relation to the 16 mandatory controls

Closing the gaps
Set up a project with the aim of closing the gaps

Starting

Getting started
Your swift.com administrator logs in to the KYC Registry Security Attestation Application (KYC-SA) and assigns permissions to business users

GO

Deciding who does what
Business users decide who will input the attestation data – the 'submitter' – and decide who will sign off the submission – the 'approver'

Attesting

Drafting your report
The submitter inputs your status for each of the controls

Approving and submitting
The approver reviews and formally signs off the submission to SWIFT

SWIFT qualification
SWIFT reviews and qualifies your submission

Staying ahead

SWIFT publishes your attestation
SWIFT publishes your attestation on the KYC-SA

Controlling who can see what
You control who can see your attestation details by allocating permissions to counterparties

You can request to see your counterparties' attestations

Reaping the benefit
Use the available information to inform your counterparty risk management processes

2

Your counterparts
Prevent and detect

There are a number of actions you can take to help manage security risk in your relationships with your counterparts that will help prevent and detect fraud.

RMA
A basic starting point is to check that you are only doing business with trusted counterparts. SWIFT's Relationship Management Application (RMA) supports customers by enabling them to control their counterparty relationships over SWIFT, by providing a pre-transaction check that prevents unauthorised receipt of transactions. SWIFT offers a number of products and services to help financial institutions optimise the use of RMA and RMA Plus in order to better understand, manage and mitigate operational, compliance and fraud risks.

https://www.swift.com/insights/news/rma-and-rma-plus_managing-correspondent-connections

Daily Validation Reports
Consider subscribing to Daily Validation Reports. This service is designed to help institutions strengthen their existing fraud controls by providing a simple and independent means of verifying their messaging activity. Daily Validation Reports is a secondary fraud control to check on transaction activity, and to provide a focused review of large, unusual and new payment flows. The reports are available next day.

www.swift.com/dailyvalidationreports

Market practice
Market practice has an important role to play in handling counterparty relationships. The 2016 SWIFT information paper "Mitigating fraud risk through strengthened payment operations" underscored the need to examine message confirmations and end-of-day statements, and outlined good practices for checking settlement instructions and changing payment instructions. Subsequently in 2017, the Payments Market Practice Group (PMPG) established Market Practice Guidelines for the cancellation of suspected fraudulent transactions.

www.swift.com/pmpg

Payment Controls
In 2018, SWIFT will launch a new Payment Controls service to complement and strengthen its customers' existing fraud controls. This new fraud and cyber-crime prevention service will enable SWIFT customers to screen their payment messages according to their own chosen parameters, enabling them to immediately detect any unusual message flows before transmission. The service is initially targeted at smaller institutions, smaller subsidiaries of larger institutions and central banks. It will be launched as a hosted utility solution, that will allow SWIFT users to access it instantly, with no hardware or software installation or maintenance.

www.swift.com/paymentcontrols

Daily Validation Reports

Activity Reporting
Transactions
Currency
Country
Counterparts

Risk Reporting
Largest transactions
Largest counterparts (BIC8)
New counterparts (BIC8)
Out-of-hours transactions

Payment Controls will allow SWIFT users to receive instant alerts to detect unusual message flows

Know your counterparts' security status.

Know cyber.

3

Your community
Share and prepare

The financial industry is global, and so are the cyber challenges it faces. What happens to one organisation in one location can be replicated by attackers elsewhere, so it is important to address cyber-defence with a global community effort.

SWIFT introduced a dedicated Customer Security Intelligence team that shares the latest anonymised information on Indicators of Compromise (IOCs) and details the modus operandi used in known attacks. Issuing such information has already made a tangible difference in the fight against fraud.

SWIFT has introduced a 'SWIFT ISAC' global information sharing portal to share detailed and technical intelligence to allow the community to protect itself, to take mitigating actions, and to defend against further attacks.

We strongly recommend that you subscribe and use the SWIFT ISAC portal to stay informed of the latest updates.

SWIFT is regularly informing its customers of relevant cyber intelligence, new market practices and recommendations. Specifically, SWIFT has built a CISO network and is engaging with the CISO community to increase collaboration and information sharing.

www2.swift.com/isac

Steps to take

Secure your local environment

Stay up to date with software

Review your fraud prevention and detection measures (including your RMA relationships)

Sign up and make use of the SWIFT ISAC information sharing portal

Provide contact details of your institution's CISO in the KYC-SA

Always inform SWIFT immediately if you suspect a cyber-attack on your SWIFT-related infrastructure.

Get in touch with SWIFT

24/7 dedicated CSP support (also to report an incident)

www.swift.com/contact-us/support

News, updates and documentation on the CSP

www.swift.com/myswift/customer-security-programme-csp

KYC Registry Security Attestation Application (KYC-SA) information and login

www.swift.com/the-kyc-registry-security-attestation-application

Security attestation support page

www2.swift.com/myprofile/res/subjects/kycsa/index.html?source=myswiftuhb

Interactive training – SWIFTSmart

www.swift.com/our-solutions/services/training/swiftsmart

Find your nearest SWIFT office

www.swift.com/contact-us

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.

For more information,
visit www.swift.com
or follow us on Twitter:
@swiftcommunity
and LinkedIn: SWIFT

Disclaimer

The information in this publication may change from time to time. You must always refer to the latest available version.

February 2018, 57341