Keeping compliant with the SWIFT CSP

CONTROL 2.9 - HERE'S WHAT YOU NEED TO KNOW

SWIFT CSP in a nutshell

In response to the increasing and complex nature of fraud and financial crime attacks across our community, SWIFT launched the Customer Security Programme (CSP) in 2016. This programme was introduced to protect organisations and the entire SWIFT ecosystem from internal and external bad actors. The SWIFT CSP is updated annually to align with the evolving threats, and this year is no different.

What's new for 2022?

The SWIFT Customer Security Control Framework (CSCF) v2022 comprises 32 controls, of which 23 are mandatory and 9 are advisory. Notably, there is one new advisory control (1.5A Customer Environment protection) and one control has been promoted from advisory to mandatory (2.9 Transaction Business controls).

With the global losses of payment fraud tripling from $9.84 billion in 2011 to $32.39 in 2020, and forecast to exceed $40 billion by 2027, control 2.9 is needed to mitigate the increased risk of payment fraud.

However, with all the noise and speculation surrounding control 2.9, we're here to clarify what it entails and why it's important to you and your organisation.

A deep dive into the new mandatory control 2.9

In a bid to protect the SWIFT network, all users must now implement effective detection, prevention, and validation solutions to ensure that their transactions occur within the bounds of normal business activities.

This is a significant change for the entire financial services community as it addresses the seriousness of the threat landscape and provides a solution for organisations to stay one step ahead of fraudsters. This is especially important as fraudsters are increasingly using machine learning (ML) to camouflage their fraudulent schemes under the guise of normal business activity.

SWIFT's definition of Control 2.9 'ensure outbound transaction activity within the expected bounds of normal business'

bottomline.com

But what is 'normal' business?

This is a difficult question to define, but what's certain is that there isn't a simple or blanket answer. Instead, defining normal business must be done on an organisation-by-organisation basis.

Here's how can we help

Our Secure Payments CSP solution is designed to understand your business by monitoring user activities to build a clear and complete picture of normal behaviour. In addition to using machine learning and rule-based analysis to provide real-time alerts of suspicious payments made on the SWIFT network.

Secure Payments CSP ensures transactions are conducted within the expected bounds and limits. You can...

- use machine learning, business rules and behaviour profiling to monitor transaction and user activity.

- identify threats in real-time to review and stop suspicious transactions before they leave your business.

- monitor, alert and stop anomalous actions on the SWIFT network.

- learns and adapts to emerging threats.

- comply with the existing mandatory control 6.4

To find out more please speak to your account manager or contact us.

CONTACT US

![Bottomline logo] **Bottomline**®

Connect with us

Corporate Headquarters
325 Corporate Drive
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
Fax: +1-603-436-0300
info@bottomline.com

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
Fax: +44-118-982-2253
emea-info@bottomline.com

Asia Pacific Headquarters
Level 3, 69-71 Edward Street
Pyrmont, Sydney NSW 2009
Australia

Tel: +61-2-8047-3700
Fax: +61-3-9824-6866
apac-info@bottomline.com