Customer Security Programme (CSP)

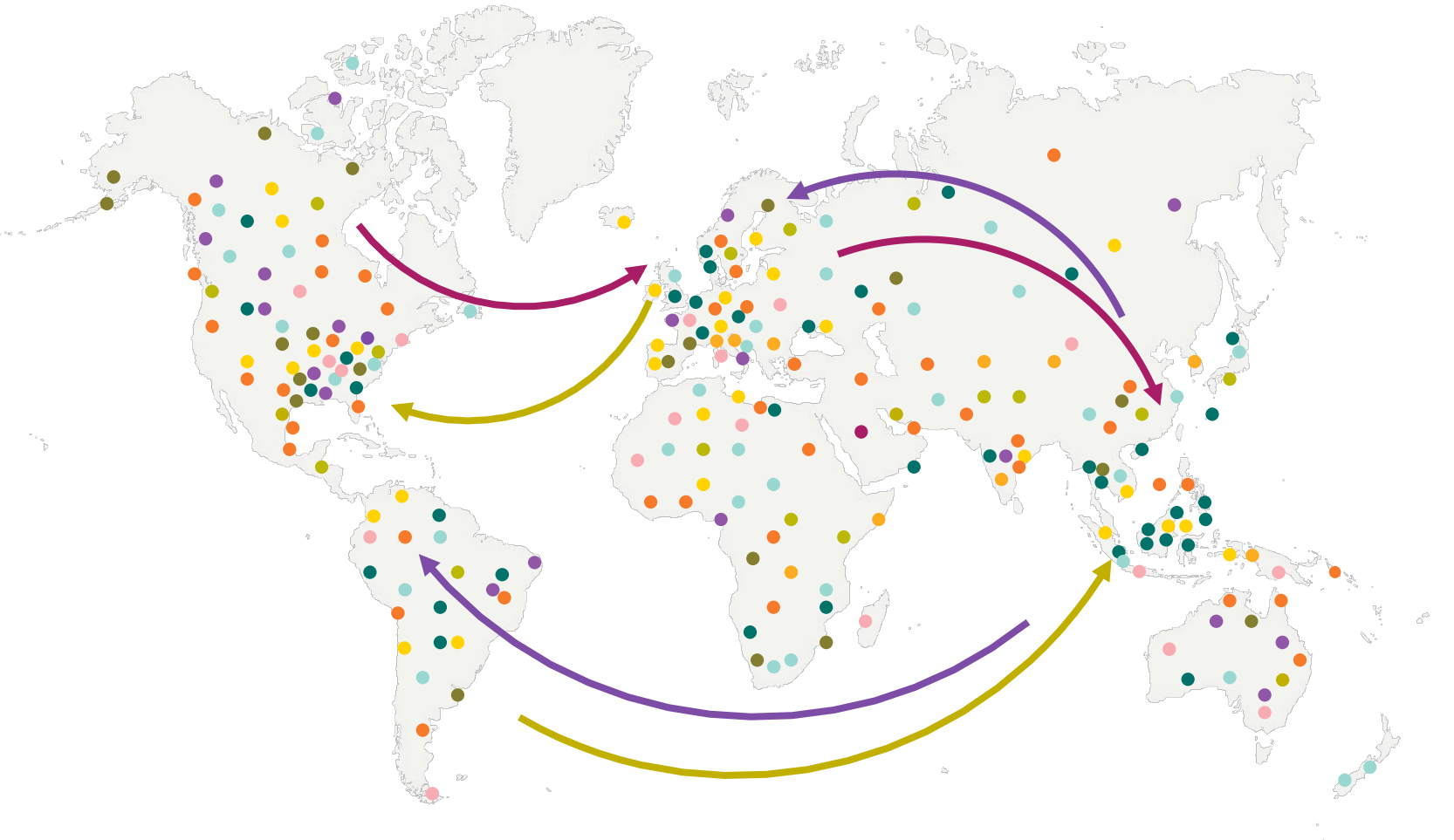
ACSDA General Assembly | Overview

Thomas Trépanier

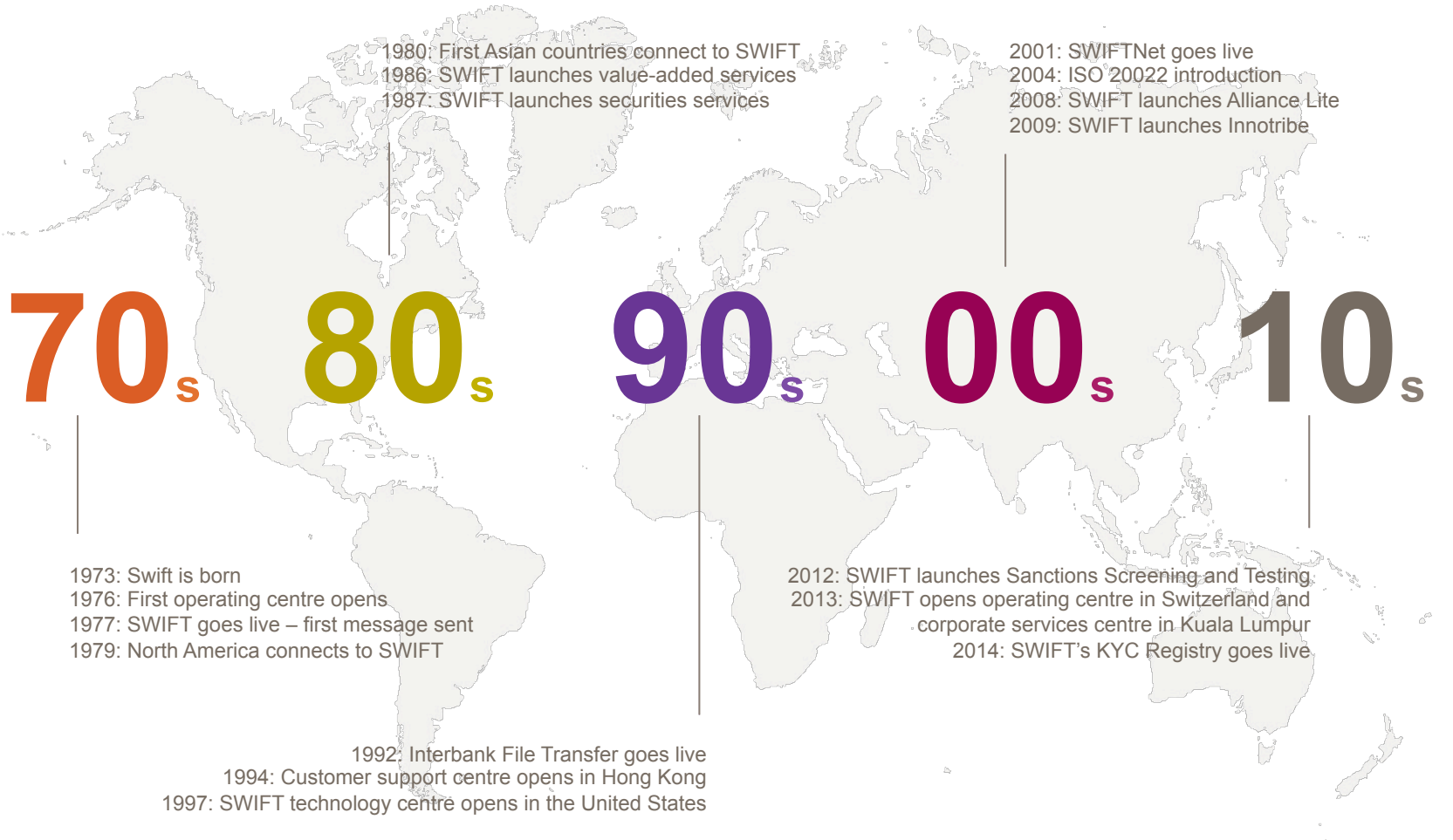
April - 2017

Legal Notices:

The global provider of secure financial messaging services



40 years serving the global financial community



70s

1973: Swift is born
1976: First operating centre opens
1977: SWIFT goes live – first message sent
1979: North America connects to SWIFT

80s

1980: First Asian countries connect to SWIFT
1986: SWIFT launches value-added services
1987: SWIFT launches securities services

90s

1992: Interbank File Transfer goes live
1994: Customer support centre opens in Hong Kong
1997: SWIFT technology centre opens in the United States

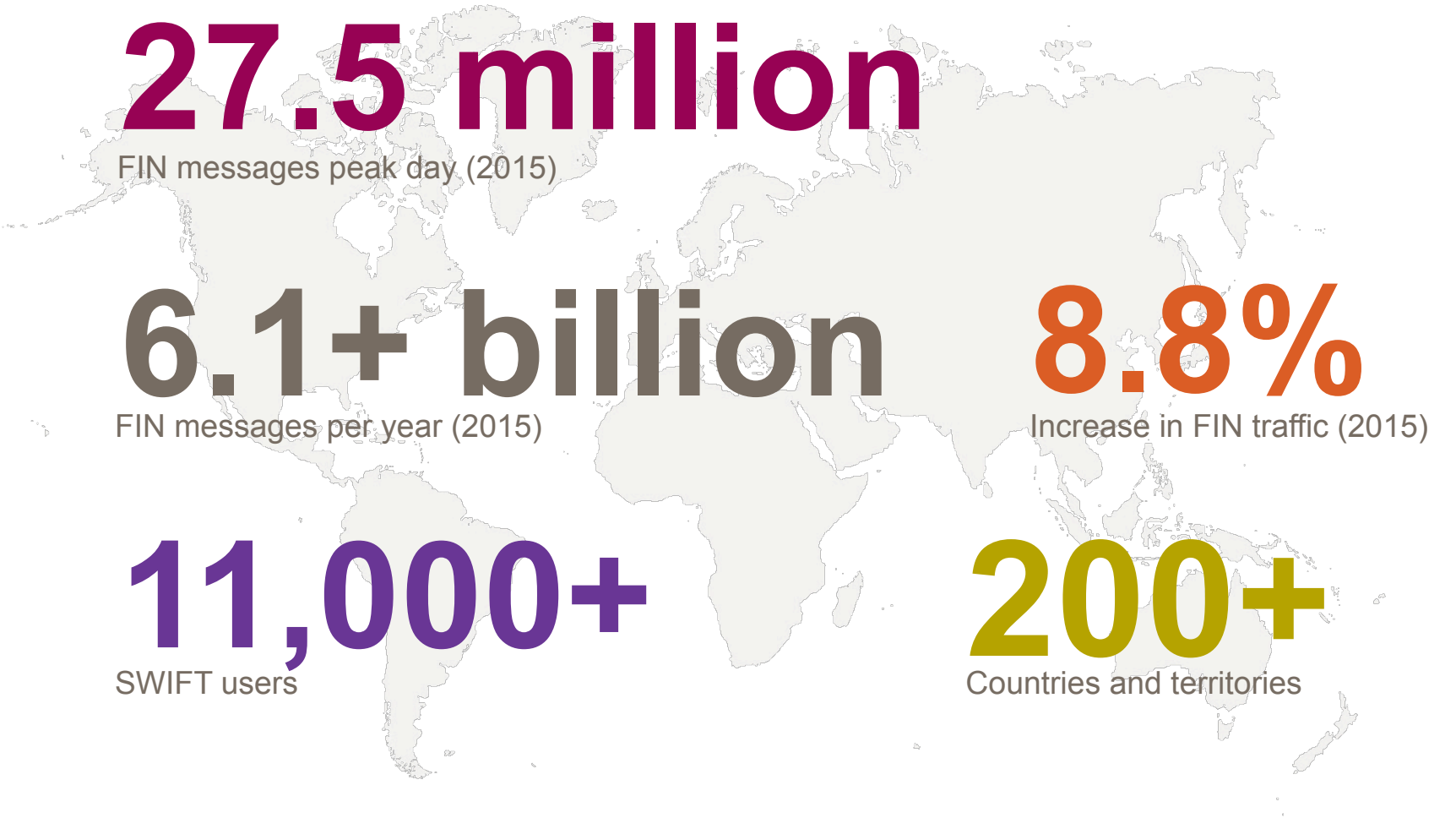
00s

2001: SWIFTNet goes live
2004: ISO 20022 introduction
2008: SWIFT launches Alliance Lite
2009: SWIFT launches Innotribe

10s

2012: SWIFT launches Sanctions Screening and Testing
2013: SWIFT opens operating centre in Switzerland and corporate services centre in Kuala Lumpur
2014: SWIFT's KYC Registry goes live

SWIFT in figures



27.5 million
FIN messages peak day (2015)

6.1+ billion
FIN messages per year (2015)

8.8%
Increase in FIN traffic (2015)

11,000+
SWIFT users

200+
Countries and territories

SWIFT users


Banks
Fund Managers
Central Counterparties
Clearing & Settlement Systems
Corporates
Broker-Dealers
ICSDs
Central Banks
Global Custodians
CSDs
Stock Exchanges
Depositories
Trade Repositories

SWIFT 2020 – strategic priorities

SWIFT 2020 – strategic priorities

Messaging

Integration & Interfaces

Shared Services

Cyber Security

Why is it important? Cyber challenges are here to stay

Central Banks To Review Security For Wholesale Payments

By **Melissa Lipman**

Law360, London (September 16, 2016, 6:49 PM BST) -- A group of central bankers plans to review security procedures for wholesale payments involving financial institutions in light of growing concerns over cyber fraud, the Bank for International Settlements said Friday.

The BIS' Committee on Payments and Market Infrastructures — a global standard-setting body for payment, clearing and settlement services made up of central banks from G-10 countries — set up a task force to look at security used for payments involving banks, financial market infrastructures like central clearing counterparties, and other institutions.

The task force will start by reviewing the current security practices used for wholesale payments before the committee decides what to do next, according to CPMI Chairman Benoît Cœuré.

"Recent incidents of cyber fraud are of significant concern for the central banking community, and we are working to make sure there are adequate checks and balances in place at each stage of the payments process," Cœuré said. "It is premature to speculate what will result from this work."

The task force will build on other work the committee has done involving cybersecurity and efforts to bulk up financial infrastructure.

WHEN REPORTS SURFACED in February of a spectacular bank hack that sucked $81 million from accounts at Bangladesh Bank in just hours, news headlines snickered over a typo that prevented the hackers from stealing the full $1 billion they were after.

Last week the snickering stopped with new reports that the hackers struck a second bank, and possibly others—though authorities won't say if those heists were equally successful. Bank hacks have traditionally focused on stealing the login credentials of bank account holders—either individuals or small businesses. Billions have been stolen successfully in this way. But the hacks in this case targeted the banks themselves and focused on subverting their SWIFT accounts, the international money transfer system that banks use to move billions of dollars daily between themselves.

Consumers worried about falling victim to online banking fraud should consider banks that give customers card readers and avoid those which rely on text messages, according to leading security expert Graham Cluley. He was speaking as Tesco Bank continued to deal with the fallout from the "systematic, sophisticated attack" that resulted in £2.5m being taken from around 9,000 current account holders.

Meanwhile, another expert says that the Tesco attack last weekend could be the first of many, and banks should be forced by regulators to up their game.

Cyber Security - Need for Action

Generic Wire Fraud

Cyber Crime Gangs

Are professionals and run their activities like a business. The larger the potential return the more they will invest in their fraudulent activities

Wire payments are the most direct way to move high values out of a bank

27%

Institutions experienced direct wire payment fraud in 2014[1]

93% increase

Wire payment fraud between 2013 and 2014[1]

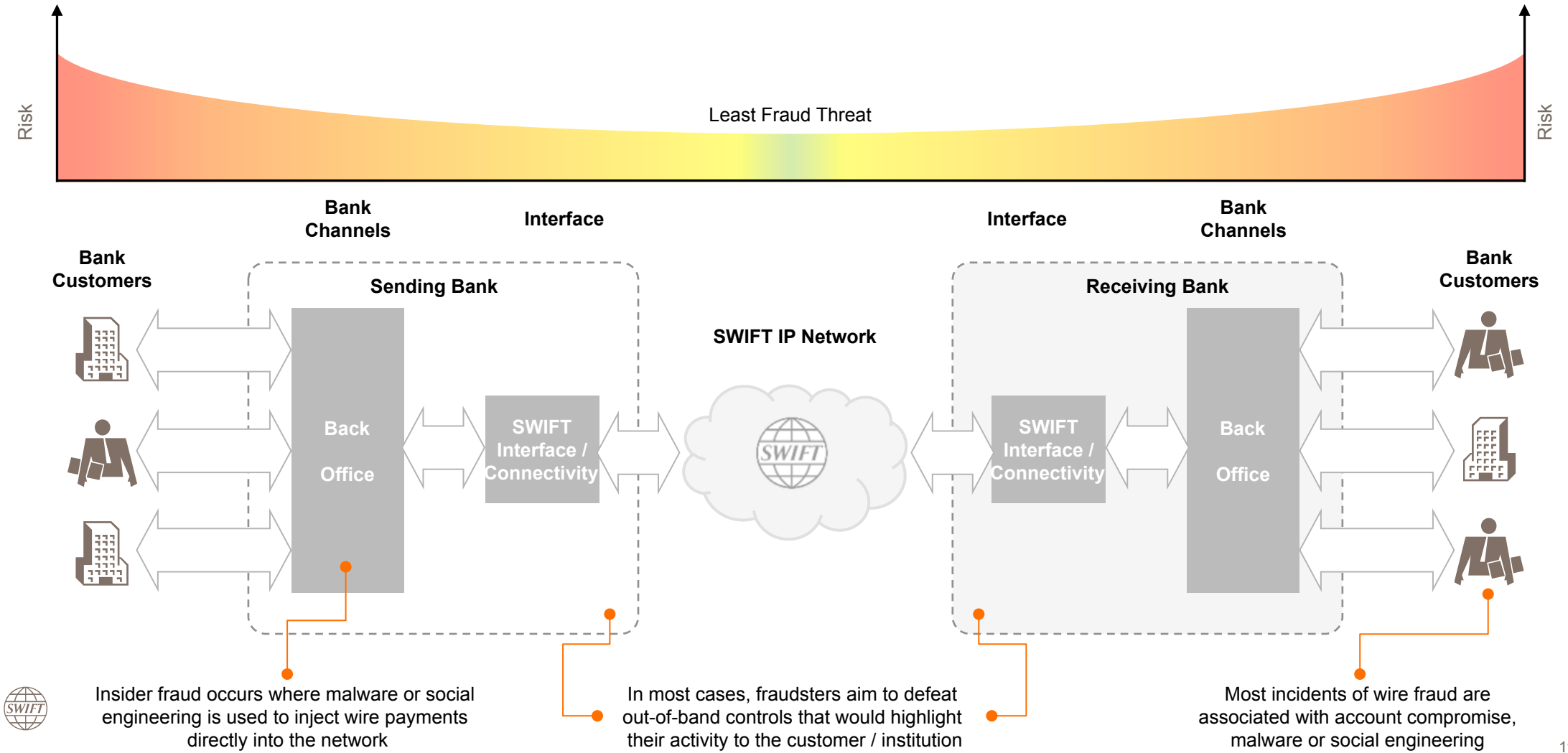
3rd most frequent

Fraud area in US after cheque and card fraud[1]

Note 1: US "Payments Fraud and Control Survey", Association of Finance Professionals, 2015

Cyber Security - Need for Action

Generic Wire Fraud



CSP | Modus Operandi

Step 1

Attackers compromise customer's environment

Step 2

Attackers obtain valid operator credentials

Step 3

Attackers submit fraudulent messages

Step 4

Attackers hide the evidence

- Attackers are well-organised and sophisticated
- Common starting point has been a security breach in a customer's local environment
- In all cases, the SWIFT's network and core messaging services have not been compromised

CSP | Framework

Customer Security Programme

While all SWIFT customers are individually responsible for the security of their own environments, a concerted, industry-wide effort is required to strengthen end-point security

In 2016, SWIFT announced its Customer Security Programme that supports customers in reinforcing the security of their SWIFT-related infrastructure

CSP focuses on mutually reinforcing strategic initiatives, and related enablers

CSP | You > Helping customers to secure and protect their local environments

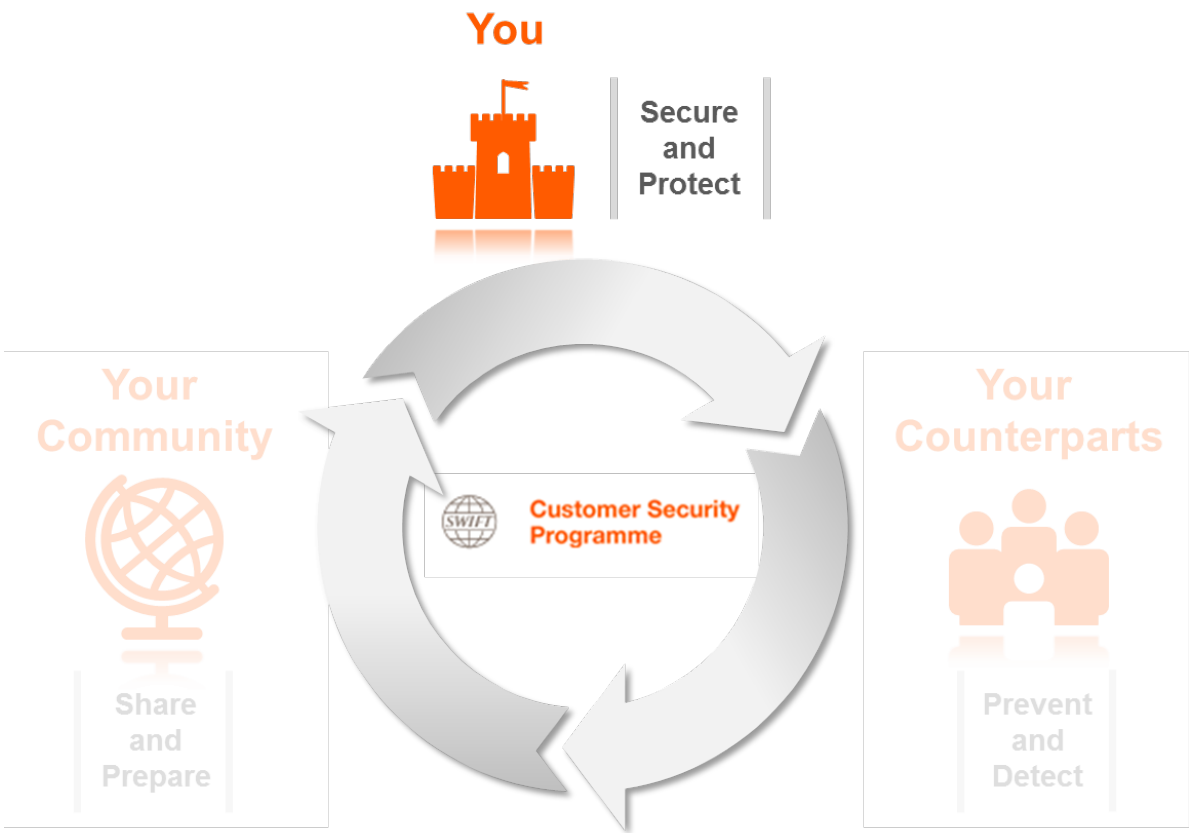
1. Security Controls Framework

2. Customer Security Attestation Process

3. Specific interface and third party security guidance documents

4. Reinforcement of SWIFT tools

CSP | You > SWIFT Tools



SWIFT Tools

- Further strengthen security requirements for interfaces, tools and software (including those from third-parties) to better protect local environments and continue efforts to harden SWIFT-provided products

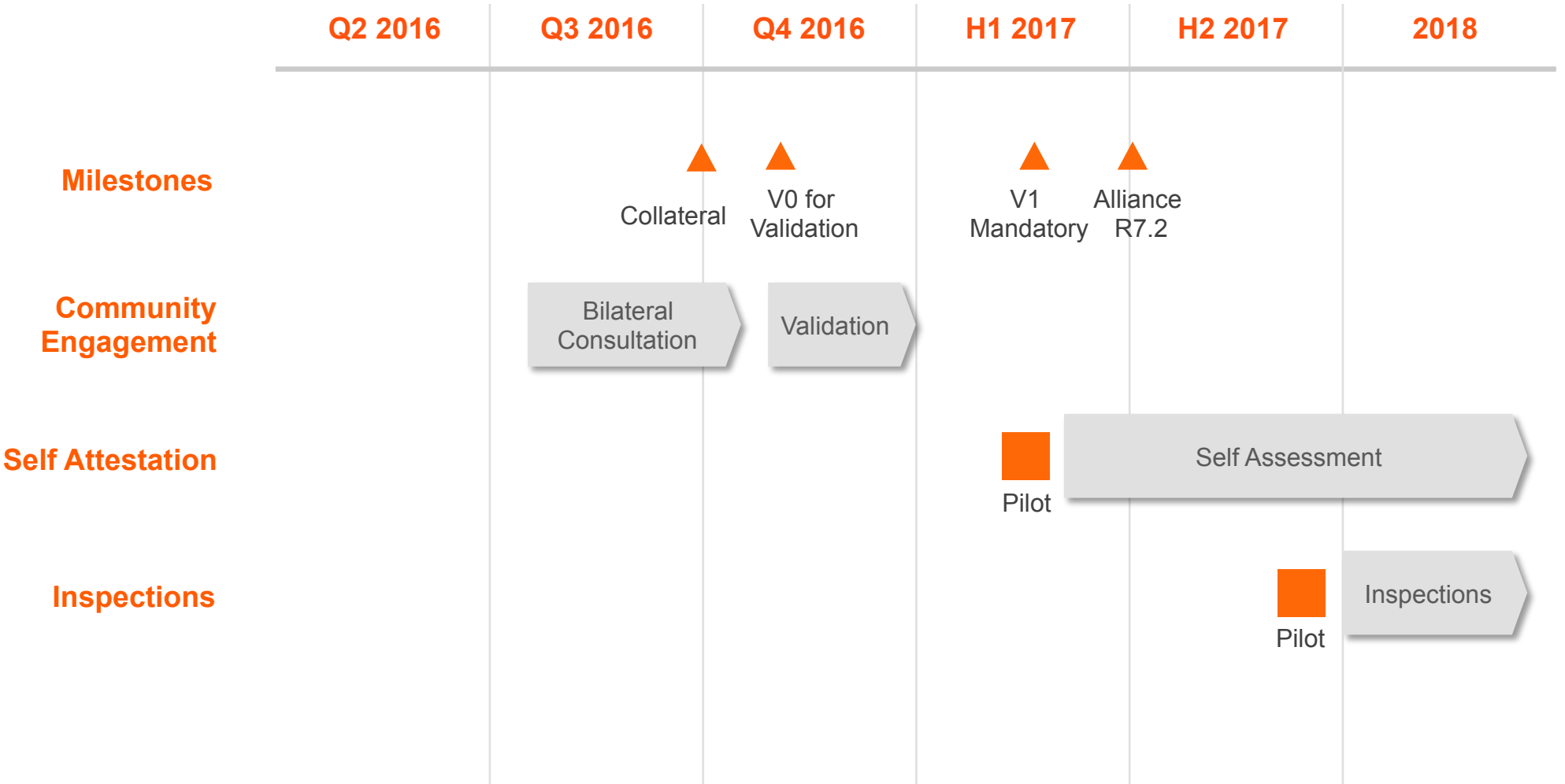
Actions to Date

- Release 7.1.14
- Release 7.1.20 and 7.0.70 with stronger default password management, enhanced integrity checking and in-built 2FA for Alliance Access clients who do not have existing 2FA implementations
- Started bilateral engagement with vendors on third-party certification for interface providers
- Release 7.0.50 for Alliance Gateway and SWIFTNet Link introducing enhanced integrity monitoring capabilities
- SAG/SNL 7.0.50 and SAA 7.1.21
- Lite2 Autoclient Q1 2017
- February Security Update (SAA 7.1.21, SAG/SNL 7.0.51) covering the complete product portfolio

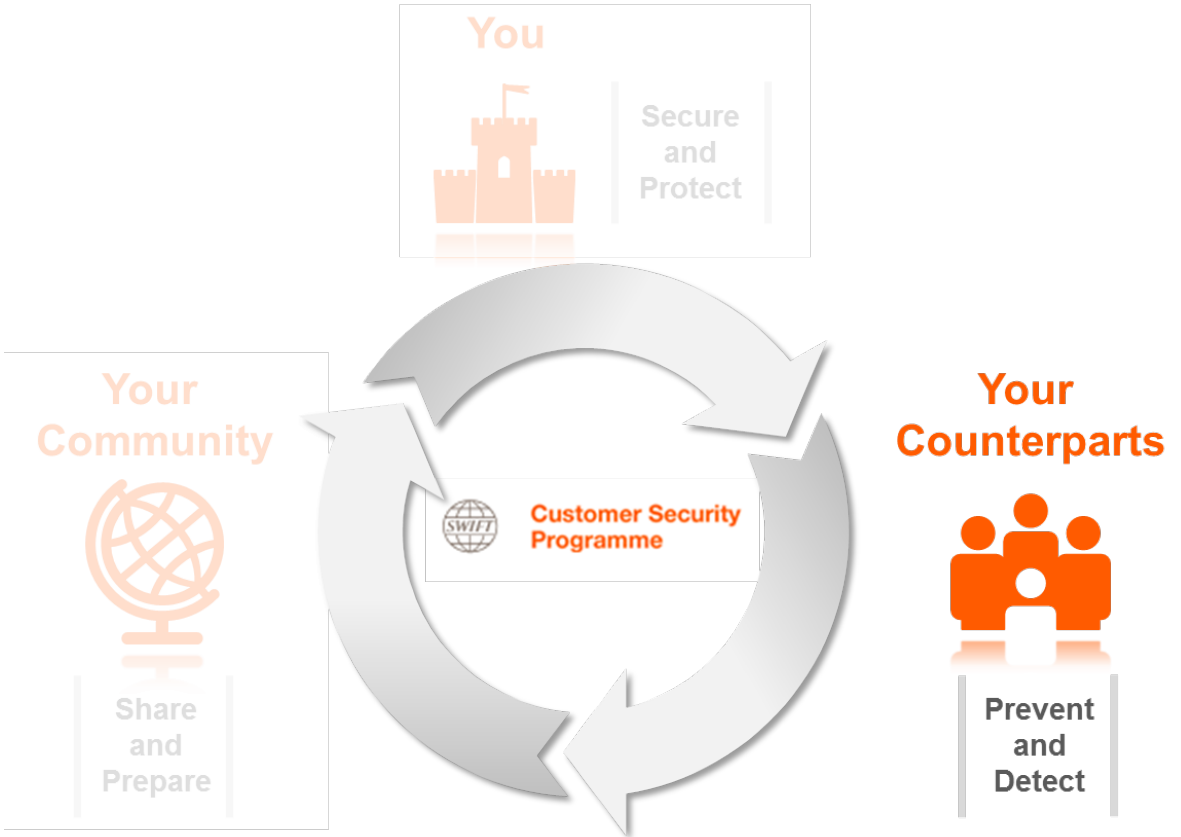
Forward planning

- AMH 3.6 Q2 2017
- Access 7.2 Q2 2017
- Focus on enforcement of mandatory updates

CSP | You > Security Guidelines and Assurance



CSP | Your Counterparts > Transaction Pattern Detection



Prevent and Detect: two primary goals

- **Enhance transaction controls:** Investigate methods to enable community to prevent and detect fraudulent transactions and identify payment risks. Pre-transaction controls, "in-flight' detection and post-transaction checks.
- **Improve market practice:** Adoption of best practice to improve community response to cyber-incidents and fraud.

Actions to Date

Enhance transaction controls:

- Pre-transaction: Launch of global RMA campaign to promote use of existing tools as a first line of defence against unwanted or unexpected message flows
- Post-transaction: 'Daily Validation Reports' launched which help customers identify possible security concerns in their daily transaction flows

Market practice:

- Information paper on best practice related to statements and cancellations

Next Steps

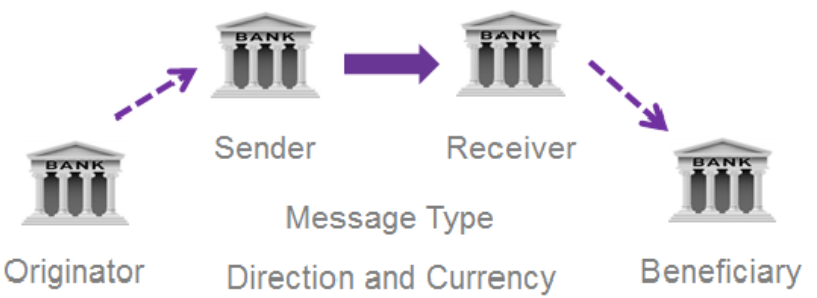
- Development of market practice for correspondent banking fraud and stopping/cancelling payments, with the SWIFT community
- Define an approach for RMA extensions
- Further exploration of "*In-flight*" payment controls

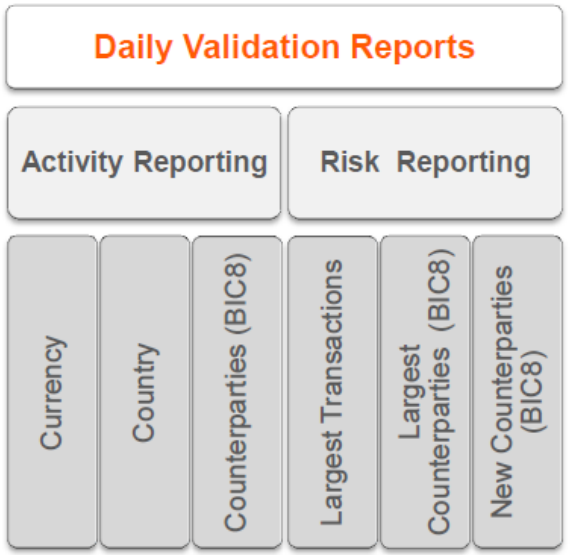
CSP | Transaction Pattern Detection - DVR

Daily Validation Reports

Activity Reporting – reports aggregate daily activity by message type, currency, country and counterparties with daily volume and value totals, maximum value of single transactions and comparisons to daily volume and value averages

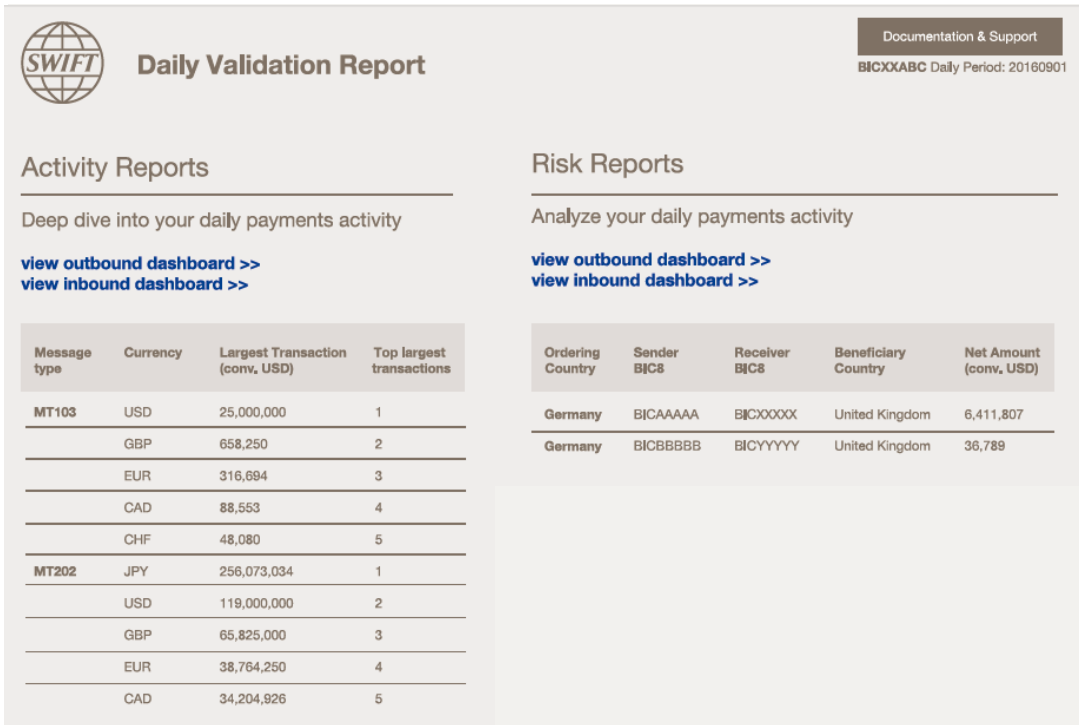
Risk Reporting - highlights large or unusual message flows based on ordered lists for largest single transactions and largest aggregate transactions for counterparties, and a report on new combinations of counterparties to identify new relationships





New Counterparties Reporting - highlights any new combinations of direct and indirect counterparties. Makes it easy to identify new payment relationships that may be indicative of risk, and helps you quickly understand the values and volumes of the transactions involved

CSP | Your Counterparts > Daily Validation Report



Daily Validation Report

Documentation & Support

BICXXABC Daily Period: 20160901

Activity Reports

Deep dive into your daily payments activity

view outbound dashboard >>
view inbound dashboard >>

Message type	Currency	Largest Transaction (conv. USD)	Top largest transactions
MT103	USD	25,000,000	1
	GBP	658,250	2
	EUR	316,694	3
	CAD	88,553	4
	CHF	48,080	5
MT202	JPY	256,073,034	1
	USD	119,000,000	2
	GBP	65,825,000	3
	EUR	38,764,250	4
	CAD	34,204,926	5

Risk Reports

Analyze your daily payments activity

view outbound dashboard >>
view inbound dashboard >>

Ordering Country	Sender BIC8	Receiver BIC8	Beneficiary Country	Net Amount (conv. USD)
Germany	BICAAAAA	BICXXXXX	United Kingdom	6,411,807
Germany	BICBBBBB	BICYYYYY	United Kingdom	36,789

Activity Reports | Aggregate Daily Activity

- Message type
- Currency
- Country
- Counterparties

- Daily volume total
- Daily value total
- Maximum value of single transactions
- Comparisons to daily volume and value averages

Risk Reports | Large or Unusual Message Flows Based on Ordered Lists

- Largest single transactions
- Largest aggregate transactions for counterparties
- New counterparty relationships

CSP | Your Community > Intelligence Sharing

Intelligence Sharing

- Deepen our cyber security forensics capabilities so that we can create unique intelligence on SWIFT-related events and disseminate anonymised information to the community

Actions to Date

- Established a Customer Security Intelligence (CSI) forensics team that has built a detailed inventory of malware, e.g. File Hashes / Indicators of Compromise / Modus Operandi / FAQs …
- Contribution of intelligence to existing organisations, such as FS-ISAC and published anonymised threat intelligence to the community
- Launched Security Notification Service
- Engagement in industry forums and on a bilateral basis with customers, at CISO and COO level
- Building a comprehensive CISO network

Next Steps

- Expand SWIFT's information sharing platforms and share best practice with the SWIFT community as well as the cyber intelligence community, e.g. ISACs/ CERTs

CSP | Your Community > Third-Party Providers

Third-Party Providers

- Structural enhancement of customer security requires the extensive support of third-party providers, e.g. security software and hardware, consulting and training, implementation services, providers of fraud detection solutions, service bureaus and auditors
- Foster a secure ecosystem through partner programmes, organisation of industry events where such providers can engage with our customers, certification programmes and other measures

Next Steps

- Extend third-party certification programmes to reflect security requirements
- Engage through industry events, Innotribe and SWIFT Institute, including Sibos

CSP | Your Community > Customer Engagement and Communications

General Actions for Customers

You

- Secure your local environment
- Sign up to our Security Notification Service
- Stay up to date with SWIFT's latest security updates
- Get ready to adopt our mandatory security requirements

Your Community

- Inform SWIFT if you suspect that you have been compromised
- Provide contact details of your company's CISO for incident escalation

Your Counterparts

- 'Clean-up' your RMA relationships
- Put in place fraud detection measures
- Engage with us on market practice

Customer Security Programme
www.swift.com/csp

Security Notification Service – **https://www2.swift.com/idm/myinfo/newsletters.faces**

CISO – Chief Information Security Officer: **https://www.swift.com/ordering-support/customer-security-programme-csp_/contact-us/ciso-registration**

CSP | Open Discussion

Questions and open discussion

www.swift.com