SWIFT update on cybersecurity

What's changed, what should banks do, how is SWIFT helping?

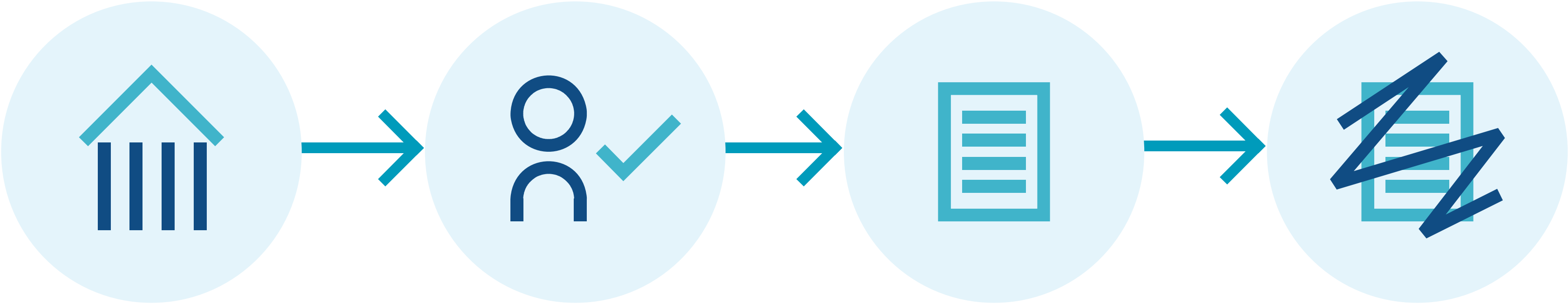
Геринг Матвей Филиппович (Matthieu de Heering)
Head of Central and Eastern Europe, SWIFT

ARB conference Cybersecurity Pannel – Sochi, Russia - September 2019

v01

What has changed?

Attacks on SWIFT members have the same modus operandi



1 Cyber attackers compromise institution's environment

+ Malware injection:
  - email phishing
  - USB device
  - rogue URL
  - insider compromise

2 Cyber attackers obtain valid operator credentials

+ Long reconnaissance period learning banks' back office processes
+ Keylogging/screenshot malware looking for valid account ID and password credentials

3 Cyber attackers submit fraudulent messages

+ Attackers impersonate the operator/approver and submit fraudulent payment instructions
+ May happen outside the normal bank working hours or over public holidays

4 Cyber attackers hide the evidence of their actions

+ Attackers gain time
  - deleting or manipulating records & logs used in reconciliation
  - wiping the master boot record

TLP:AMBER

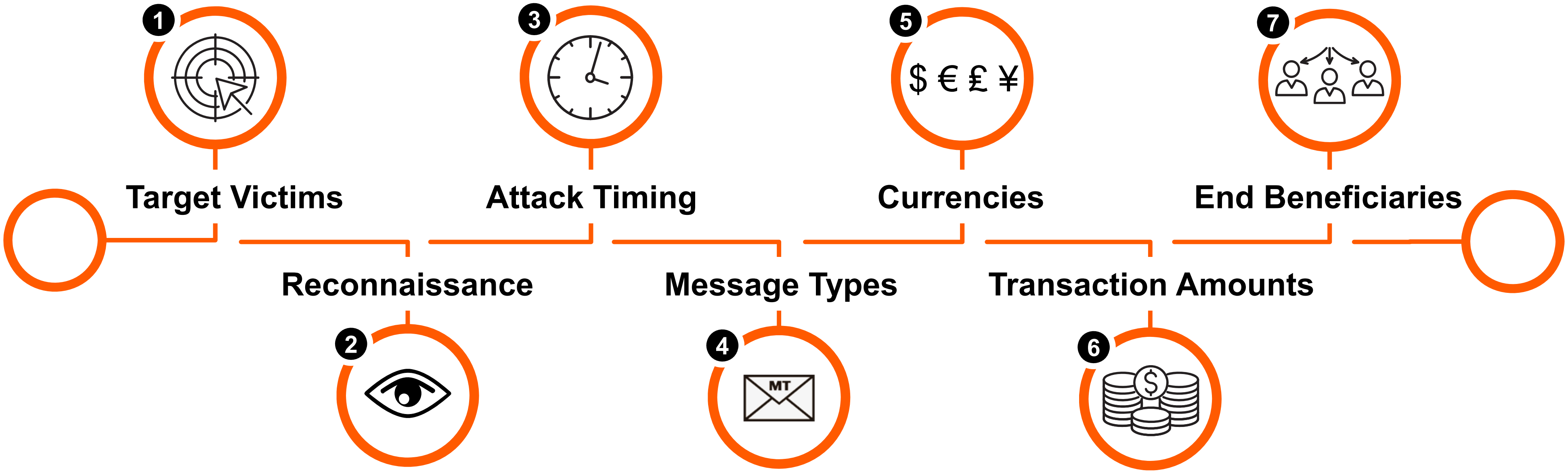
As attacks on SWIFT customers continue, a risk profile emerges of the threat

Profile of target customers:
- (Very) High on Basel AML Country Corruption Risk Index
- Central Africa, Central Asia, South East Asia, Latin America
- Banks with small traffic volumes

- Outside business hours
- During local public holidays
- During business hours to blend in with legitimate traffic
- Fraudulent messages can be minutes or hours apart

Currency of fraudulent transactions:
- 70% USD
- 21% EUR
- 9% GBP, HKD, AUD, JPY

Beneficiary destination of fraudulent transactions:
- 83% Asia Pacific
- 10% Europe
- 4% North America
- 3% Middle East



1 Target Victims

2 Reconnaissance

3 Attack Timing

4 Message Types

5 Currencies

6 Transaction Amounts

7 End Beneficiaries

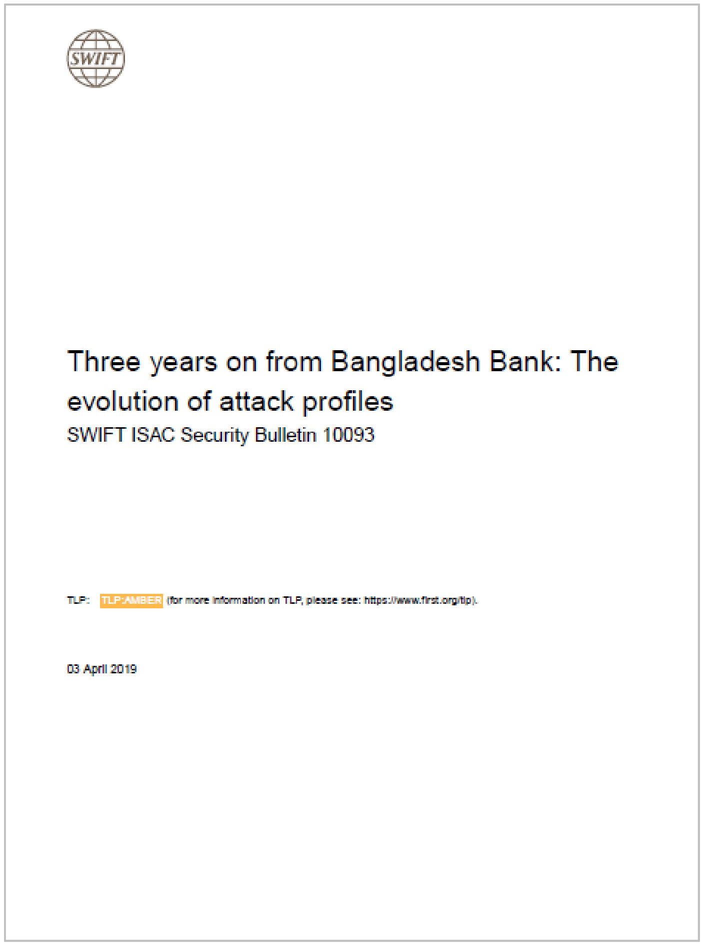
- Attacker patience – can wait for weeks / months before injecting fraudulent messages
- Reconnaissance time used to gather user credentials and learn operational behaviour

- Cross-border payments
- Mainly MT-103 FIN messages
- Typically messages are sent from victim bank to beneficiary bank via correspondent Nostro bank(s)

- Before 2018, typically MUSD ten or MUSD tens
- From 2018, typically MUSD 0.25 to 2
- Typical per transaction amounts were much larger than ‘average’ amounts sent over them in the prior 24 months

TLP:AMBER

As attacks on SWIFT customers continue, a risk profile emerges of the threat



Three years on from Bangladesh Bank: The evolution of attack profiles

SWIFT ISAC Security Bulletin 10093

TLP: TLP:AMBER (for more information on TLP, please see: https://www.first.org/tlp).

03 April 2019

SWIFT ISAC Report
April 2019

Three years on from Bangladesh

Tackling the adversaries

Detailed Bulletin 10093:

Bulletin published on SWIFT ISAC on 03 Apr 2019

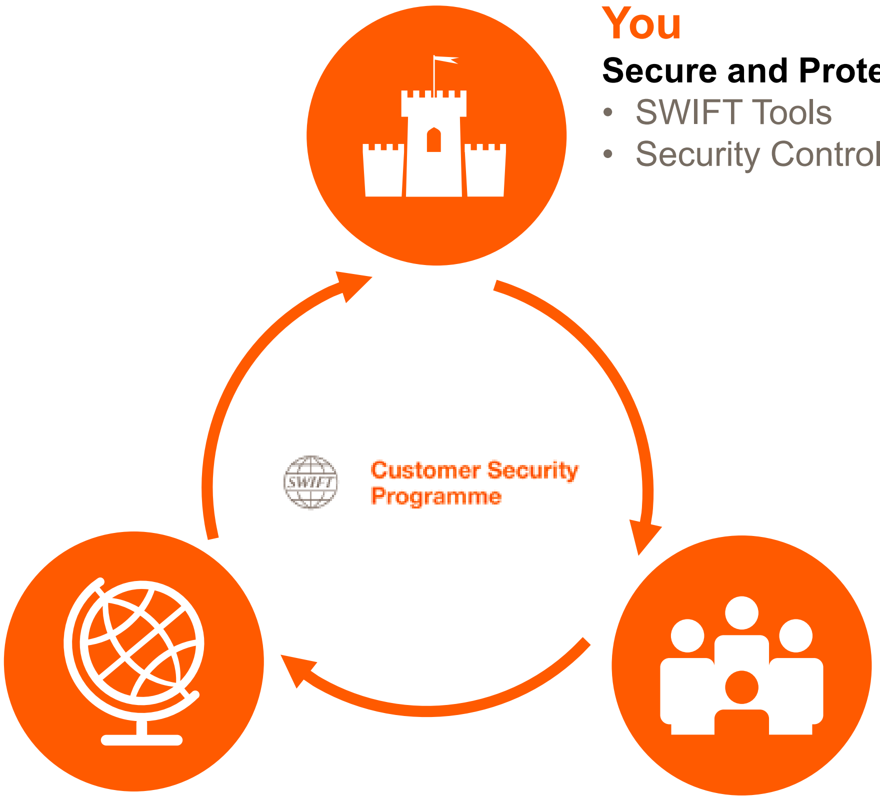
Summary White Paper:

White Paper published to community on 10 Apr 2019

What should banks do?

Customer Security Programme (CSP)

Launched in 2016, CSP is designed to help SWIFT users implement practices that are essential to help protect against, detect and share information about financial services cybercrime



You

Secure and Protect

- SWIFT Tools
- Security Controls

Your Counterparts

Prevent and Detect

- Transaction Pattern Detection
- RMA, DVR and ‘In Flight’ Sender Payment Controls Service

Your Community

Share and Prepare

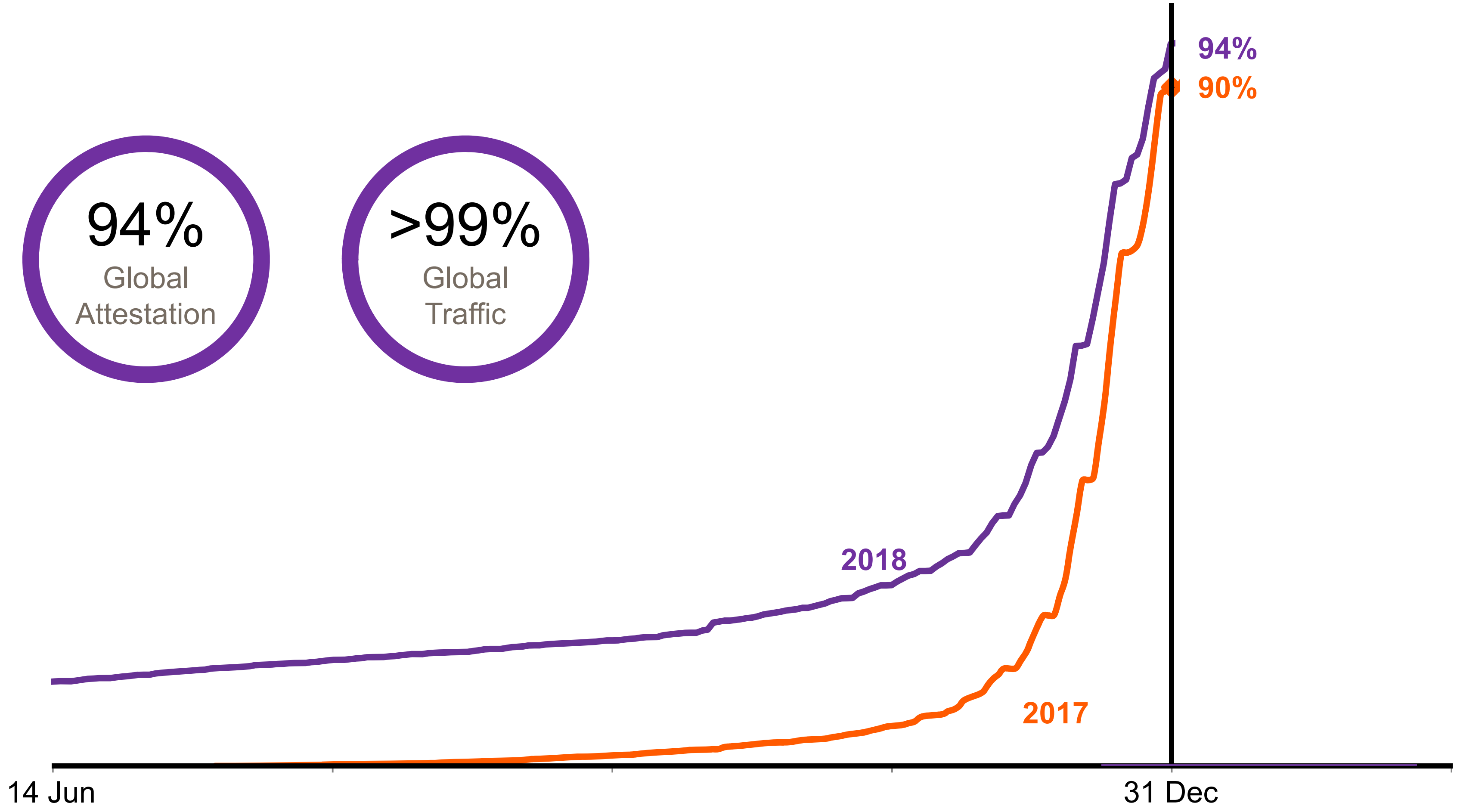
- Intelligence Sharing
- SWIFT ISAC Portal

CSP | Attestation Rates

Cumulative Count of BICs by Attestation Date – 2017 vs 2018

94%
Global Attestation

>99%
Global Traffic

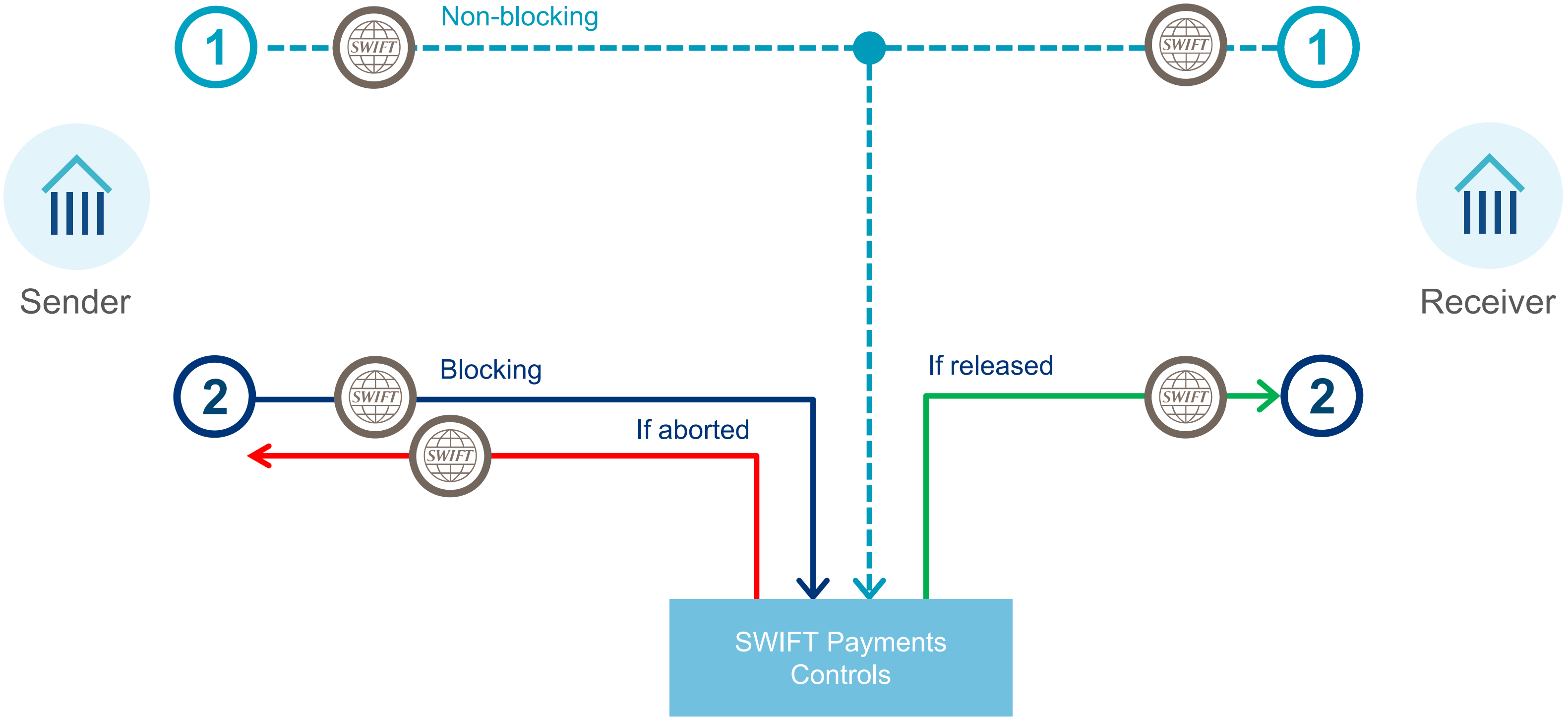


CSP | Flavours of the Independent Assessments

Assessment Type	Selection Criteria	Assessor	Timeline			
			2017	2018	2019	2020 and beyond
❶ **User-Initiated Assessment**	Voluntary - Customer Initiated	Internal or external	▨	▨	▨	▨
❷ **Community-Standard Assessment**	Mandated - All Users	Internal or external				▨
❸ **SWIFT-Mandated Assessment**	Mandated - Sampled Customers Driven by QA Analysis	External only		▨	▨	▨

How is SWIFT helping?

SWIFT Payment Controls Service - Blocking / non-blocking mode

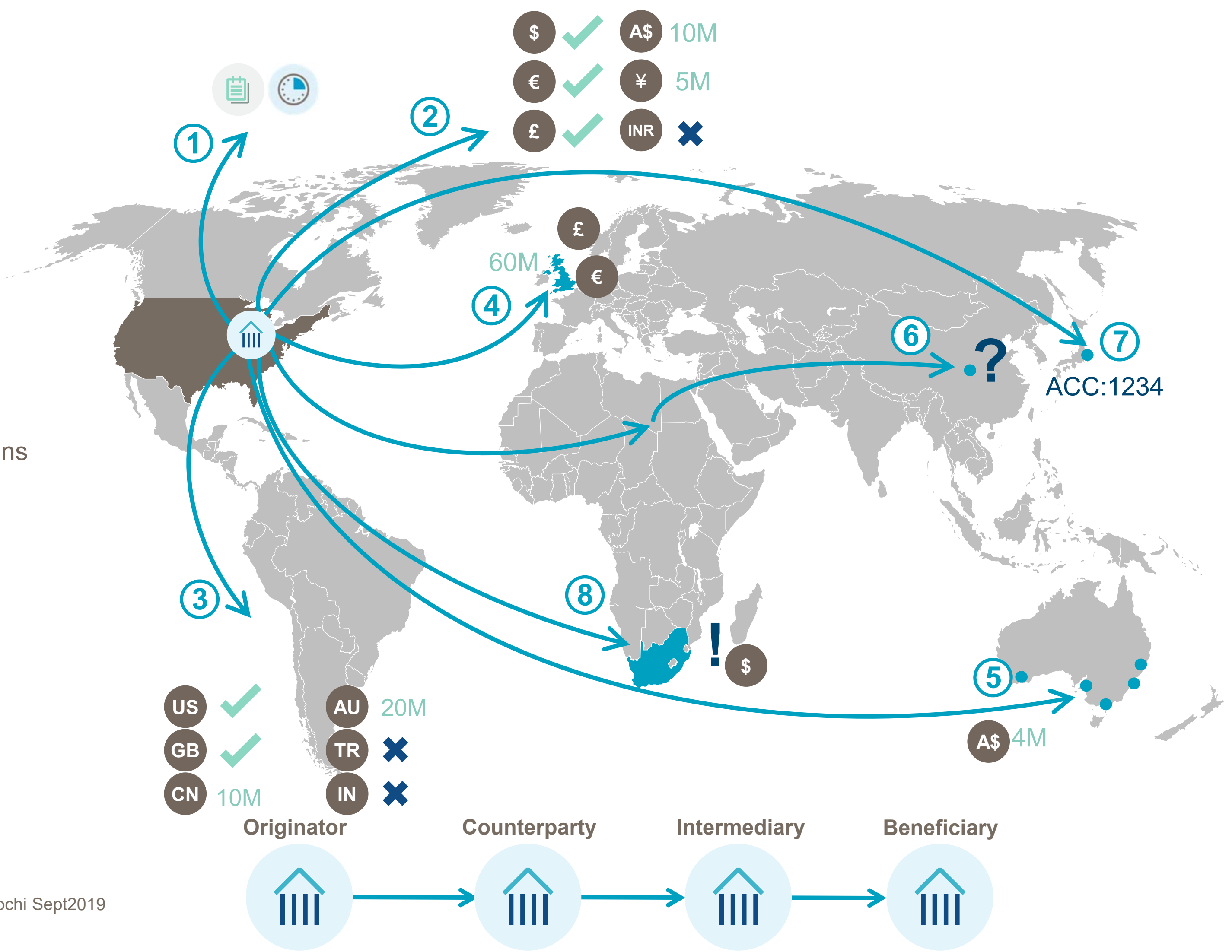


A few examples…

Flexible parameters including:

1. Business hours and days
2. Currency whitelist / blacklists, single & aggregate payment limits
3. Country whitelist / blacklists, single & aggregate payment limits
4. Country & currency threshold combinations
5. BIC & Entity institution limits
6. New payment flows
7. Suspicious accounts
8. Uncharacteristic behaviours

+ Across the complete payment chain



Specific areas of cooperation with Russian Community

Multifaceted cooperation with CBRF’s FinCERT and Rosswift

- Trilateral cooperation agreement signed (2016)
- Yearly SWIFT CSP Roadshows with introduction by CBRF
- Presentations at CBRF Magnitogorsk conference and IFC
- Active participation of RTCH head = country CISO
- Sibos plenary session
- Webinars in Russian
- Translation of CSP rule book
- Community onsite CSP Bootcamp (facilitation in RU) + individual banks’ security assessment
- Payment Controls Service Russian country deal (see next slide)

Payment Controls – special terms for Russian SWIFT users

- Designated for users with < 3’500 sent SWIFT payment messages / day
- **25% discount*** from the annual fee
- Discount application period– **through 31.12.2021**
- One-time on-boarding fee still applies

** Discount can be increased depending on tempo of Russian banks signing up*

Conclusion

Call to action for SWIFT customers

1. Stay up to date with SWIFT software releases

2. Sign up for Security Notifications and use of the SWIFT ISAC information sharing portal, which includes STIX/TAXII feeds

3. Agree bilaterally with your counterparties to consume and utilise attestation data for counterparty risk management

4. Consider SWIFT's anti-fraud tools Payment Controls, RMA clean-ups, etc.

5. Prepare and test response plan, including always informing SWIFT immediately if you suspect a cyber-attack on your SWIFT-related infrastructure

6. Ensure that you fully comply with all the CSP mandatory security controls and attest by end December

Matthieu de Heering – Геринг Матвей Филиппович

Head of Central and Eastern Europe
EMEA -- SWIFT

SWIFT HQ Belgium: + 32 2 655 3111
Belgian Mobile: + 32 495 660 396
Russian Mobile: +7 967 227 1337

Email: Matthieu.DEHEERING@swift.com

SWIFT s.c.r.l. -- Avenue Adèle 1 -- 1310 La Hulpe -- Belgium

SWIFT

www.swift.com

sibos

LONDON

23 - 26 Sep 2019

Slido