Three years on from Bangladesh

Tackling fraud with SWIFT Payment Controls

Helen Alexander, FCC Initiatives, **SWIFT**

Thomas Preston, FCC, Cyber & Screening Solutions, **SWIFT**

The Evolving Threat Landscape

Thomas Preston, FCC, Cyber & Screening Solutions, **SWIFT**
Thomas.Preston@swift.com

Rise of Cybercrime

Insights | Cybercrime

Focus of fraudsters has changed – the threat is no longer at the edge, it is at the heart

Cybercriminals are agile, creative and sophisticated

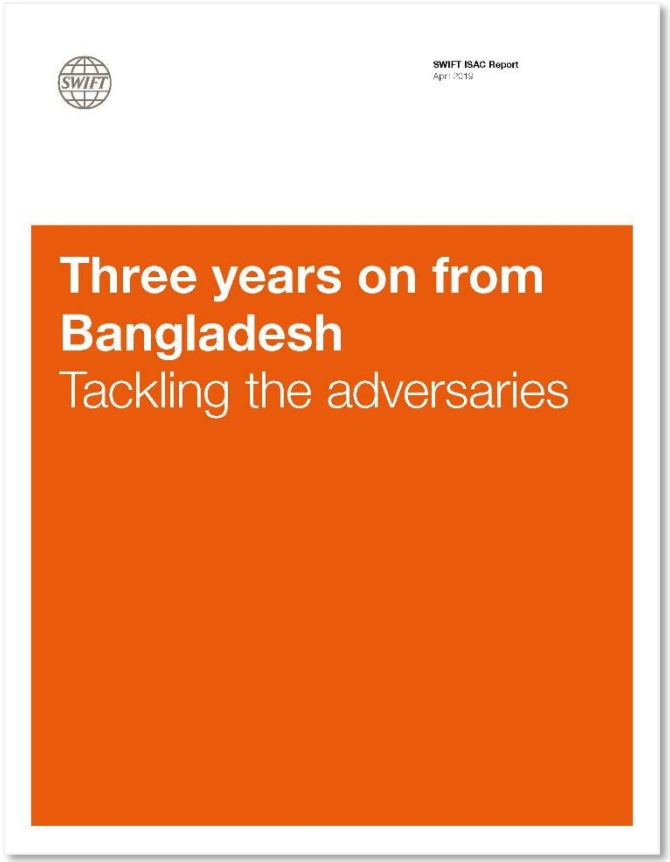
Regulators and lawmakers are waking up to the threat – 72% of jurisdictions released plans to issue new regulations on cybersecurity for the financial sector

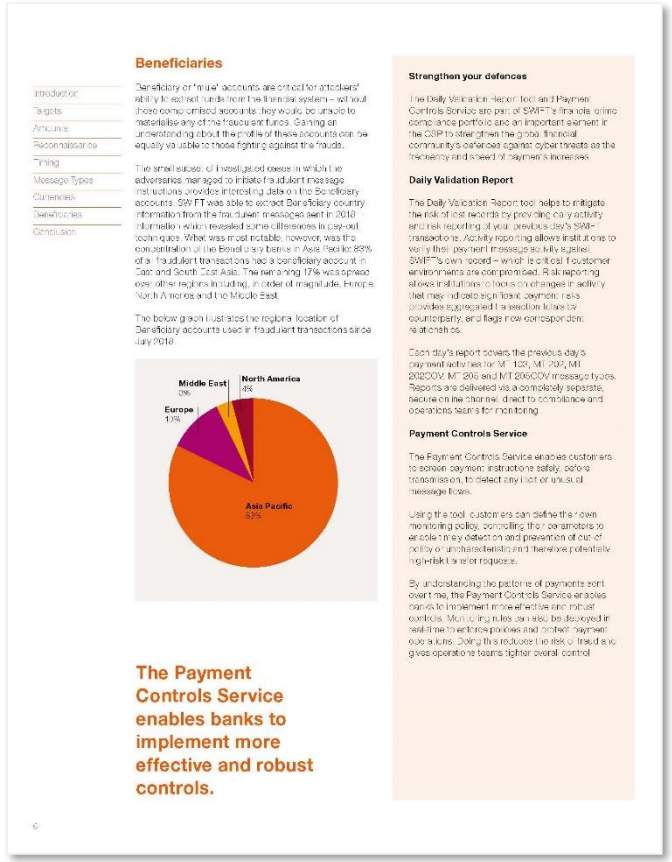
But the industry is still not as well prepared as it should be – 70% of institutions don't have a cyber incident response plan

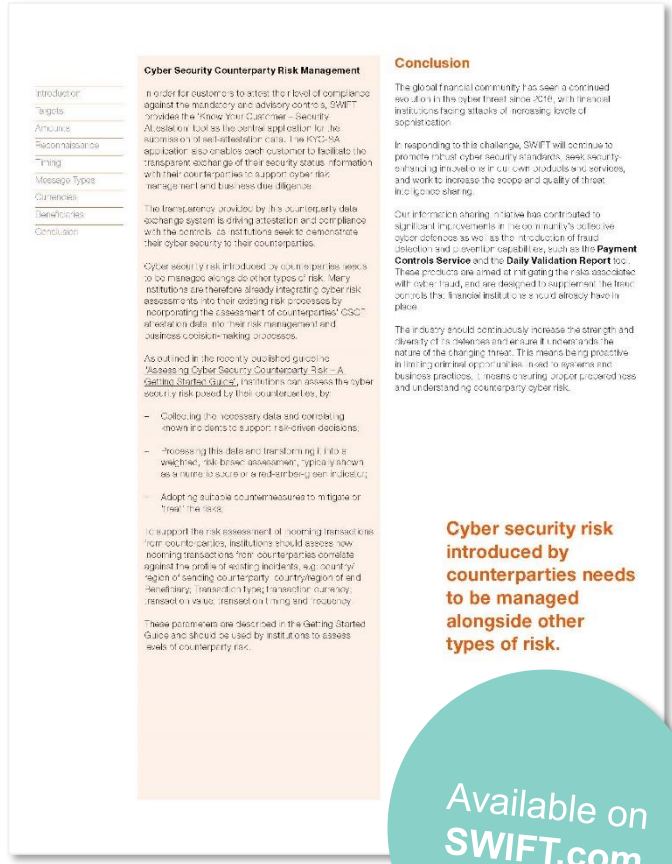
We need to work together to fight financial crime – no-one wants to be the weakest link or lose business relationships

Cyber Trends and Attack Patterns

SWIFT’s new ISAC Report

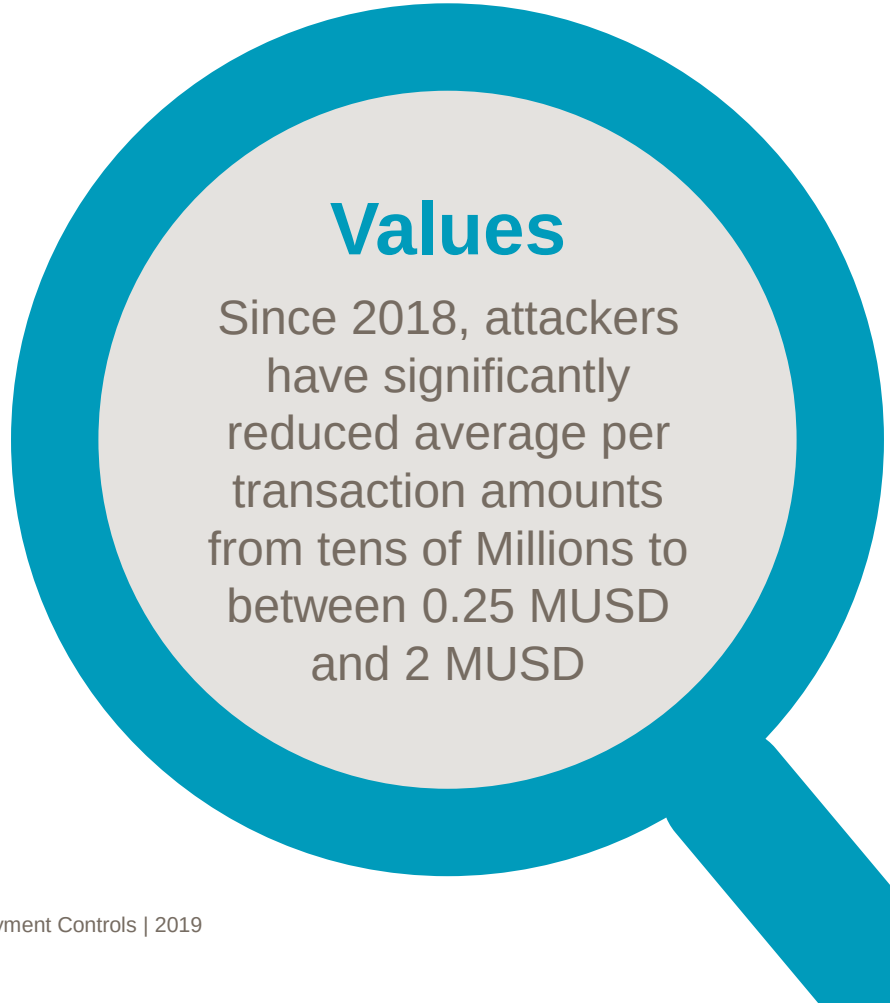






Available on **SWIFT.com**

Key Takeaways



Values

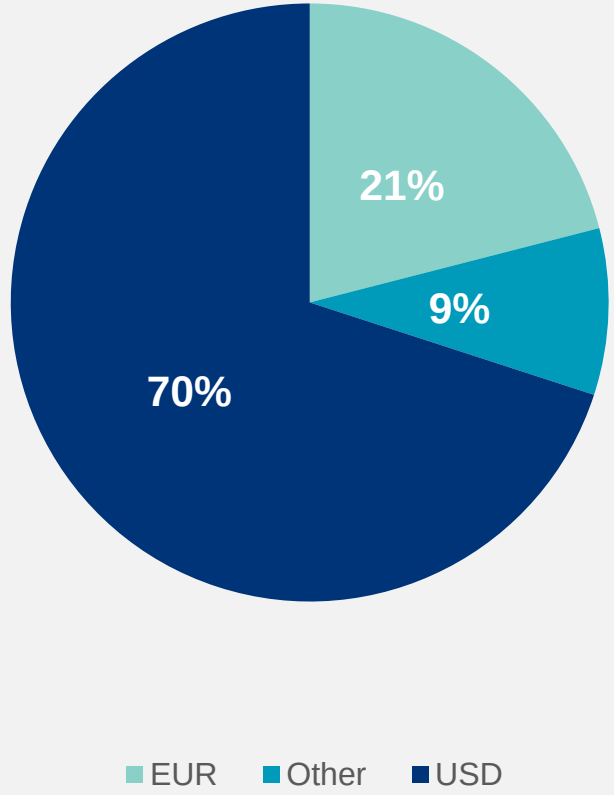
Since 2018, attackers have significantly reduced average per transaction amounts from tens of Millions to between 0.25 MUSD and 2 MUSD

Volumes

During the most recent investigations, the number of fraudulent transactions issued averaged around ten per incident within a two-hour period

Currencies

The USD accounted for approximately 70% of the fraudulent messages created since the 2016 attack. We have also observed an increased usage of European currencies – most notably EUR and GBP



Corridors

01 Fraudulent transactions were typically issued using new or dormant “payment corridors”

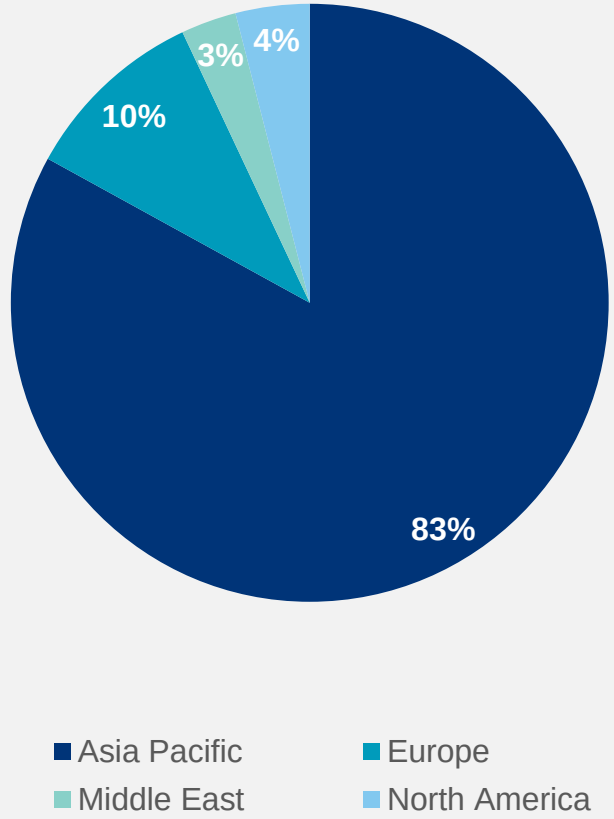
02 In the cases where existing corridors were used, we noticed large deviations in value

03 Most of the transactions issued were handled by one or two Receiver banks and were intended for the same Beneficiary country

Geographic spread

83% of all fraudulent transactions had a beneficiary account in APAC.

The below graph illustrates the location of beneficiary accounts used in fraudulent transactions in since July 2018.



Additional collateral

ISAC Article 10060, which contains more detailed information.

Protect your business with SWIFT Payment Controls

Helen Alexander, FCC Initiatives, **SWIFT**
Helen.Alexander@swift.com

Attacks on SWIFT members have the same modus operandi

Compromise institution's environment

- **Malware** injection:
  - Email phishing
  - USB device
  - Rogue URL
  - Insider compromise

Obtain valid operator credentials

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

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

Hide the evidence of their actions

- Attackers **gain time**
  - Deleting or manipulating records & logs used in reconciliation
  - Wiping the master boot record

In the event of an attack, **any** system in the institution can be potentially compromised.

Banks require **separate** controls to check and block payments.

Introducing SWIFT Payment Controls

SWIFT Payment Controls

simply and efficiently flags and intercepts suspicious payments to protect **you** and **your counterparties**

What is **Payment Controls**?

- Zero footprint, in-network payment monitoring
- Alert or block suspicious payments in real-time

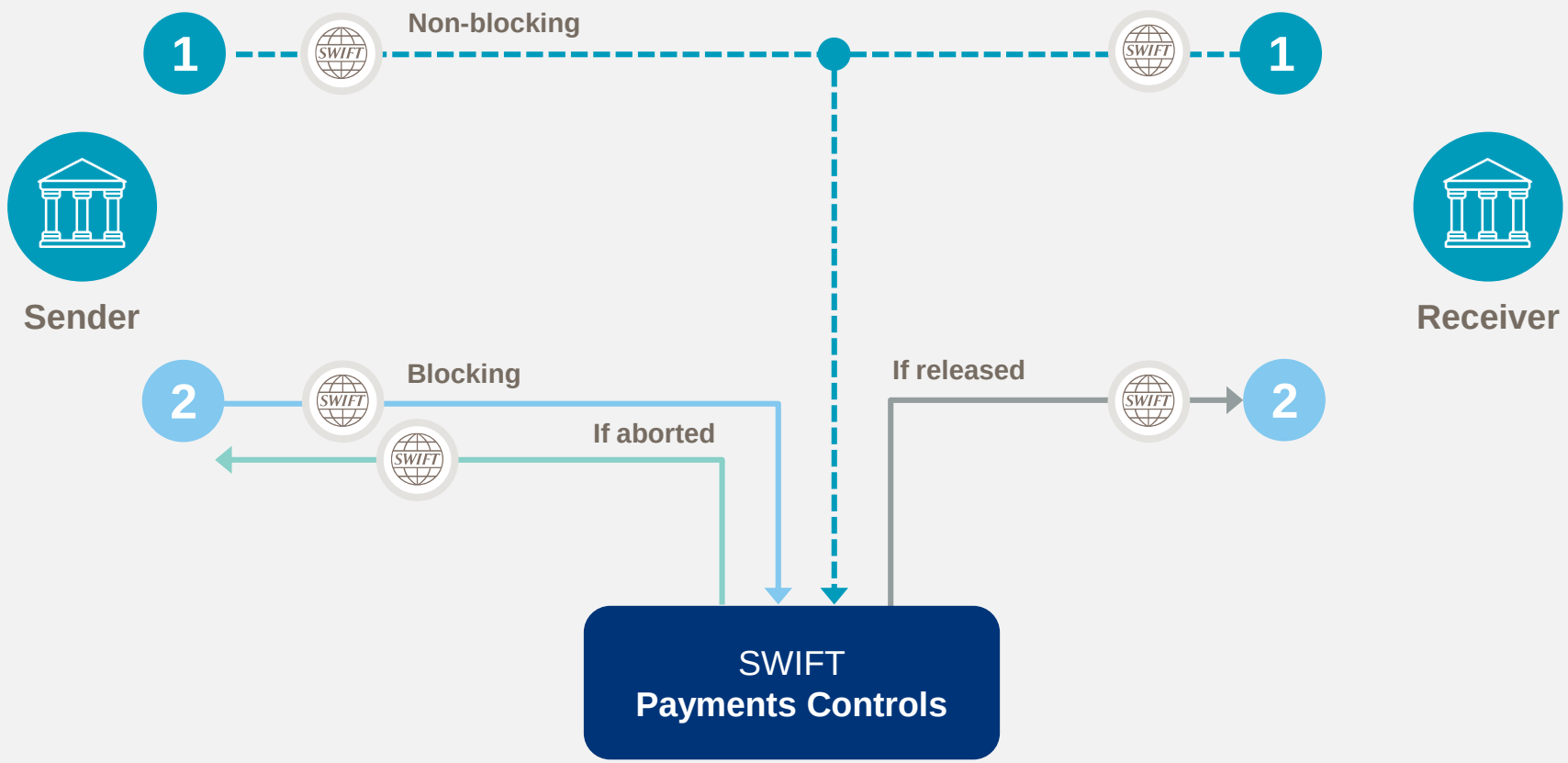
What features does **Payment Controls** offer?

- Correspondent banking focused models
- Highly subscriber-configurable
- Alert Management & workflow
- Payment release/abort
- Activity & risk reporting

What are the benefits of **Payment Controls**?

- Secondary control of payment traffic, separate from your own infrastructure
- Block fraudulent payments before they happen
- Rules configured based upon each institution's own traffic
- Leverages SWIFT & the community's knowledge and experience

Blocking / non-blocking



Payment Controls Capabilities

Business calendars

Identify payments that are sent on non-business days or outside normal business hours

New scenarios

Identify payments involving individual institutional participants, chains, countries, message types and currencies that have not been seen previously

Account monitoring

Verify end customer account numbers against institutional black lists and white lists

Threshold

Protect against individual and aggregated payment behaviour that is a potential fraud risk or falls outside of business policy

Profiling / learning

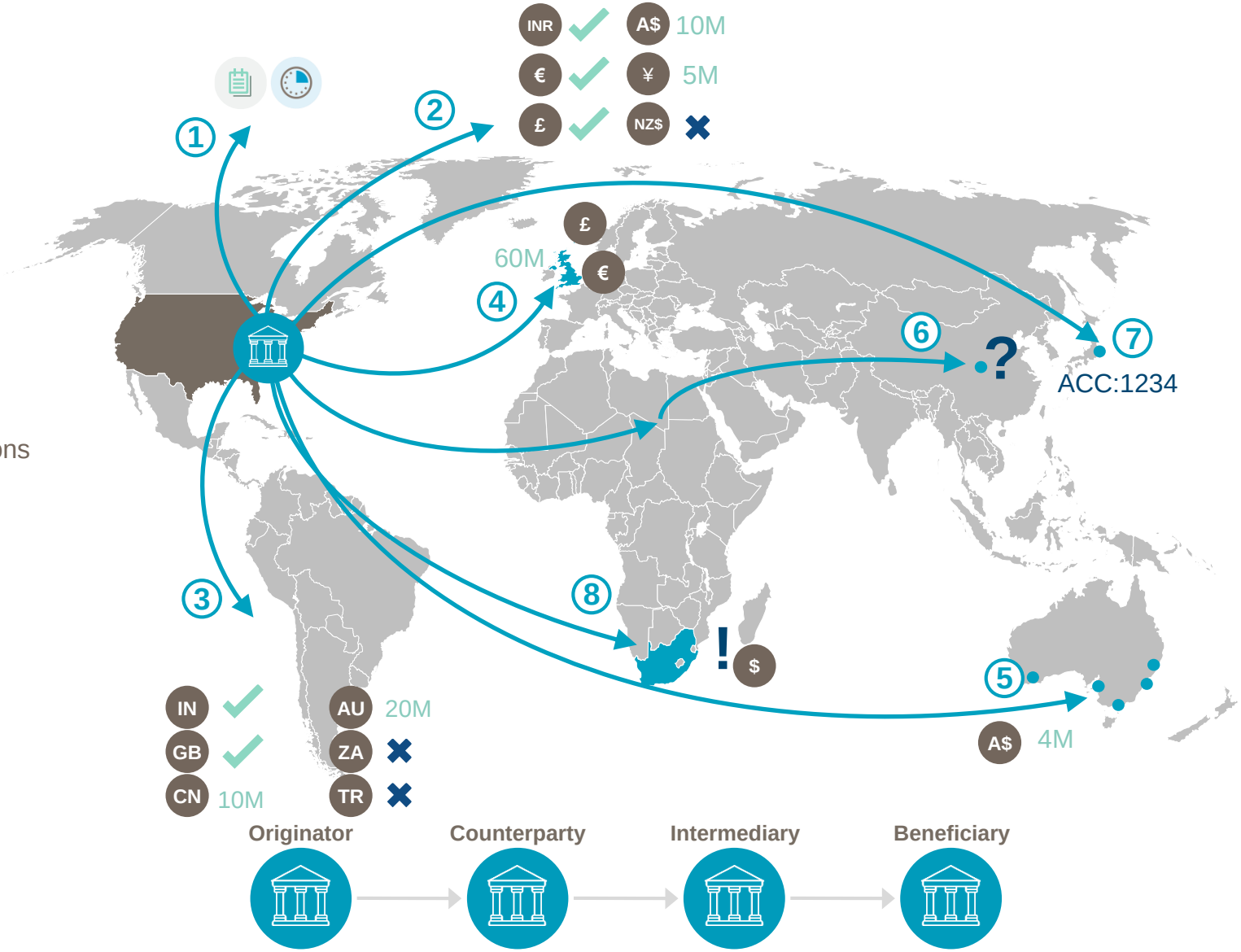
Identify & protect against payment behaviour that is uncharacteristic, based upon past learned behaviour

A few examples…

Flexible parameters including:

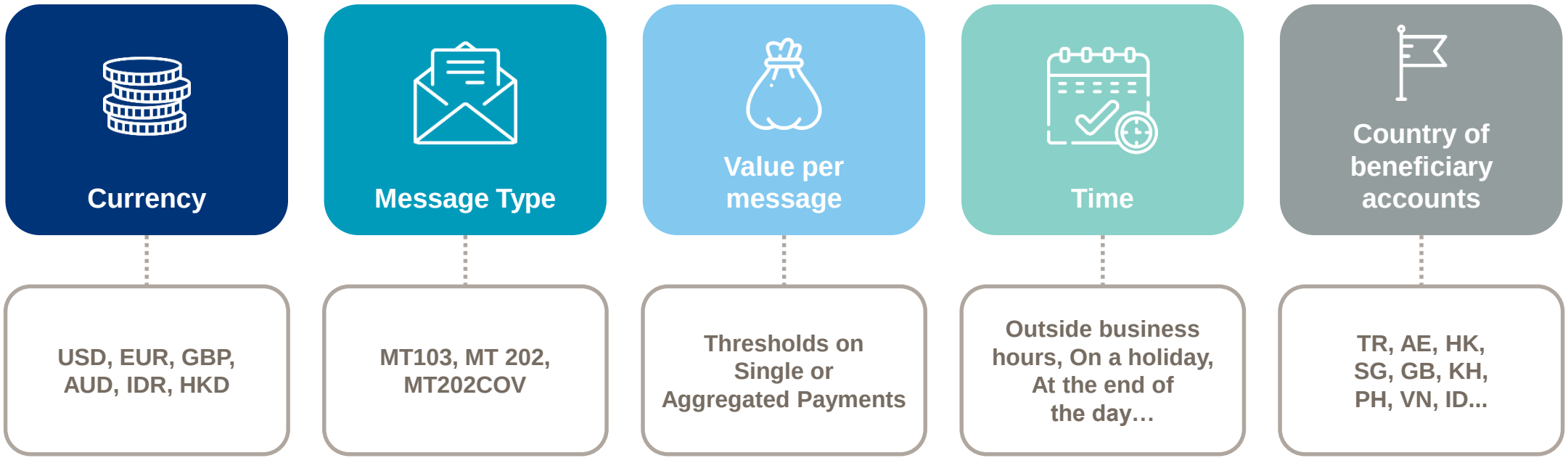
1. Business hours and days
2. Currency whitelist / blacklists, single & aggregate payment limits
3. Country whitelist / blacklists, single & aggregate payment limits
4. Country & currency threshold combinations
5. BIC & Entity institution limits
6. New payment flows
7. Suspicious accounts
8. Uncharacteristic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

\+ Across the complete payment chain



Dimensions of the fraudulent messages

Attacks are described within the ISAC in different dimensions:



Reduce fraud risks

Reduce reputational risks

Build trust

Question and Answer

www.swift.com