



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



SWIFT ISAC Report
April 2019

Three years on from Bangladesh Tackling the adversaries

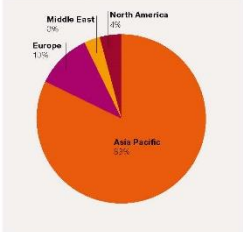
Introduction
Targets
Announce
Reconnaissance
Timing
Message Types
Currencies
Beneficiaries
Conclusion

Beneficiaries

Beneficiary of "mirai" accounts are critical for attackers' ability to extract funds from the financial system – without these compromised accounts they would be unable to monetise any of the frauds and funds. Gaining an understanding about the profile of these accounts can be equally valuable to those fighting against the frauds.

The small subset of investigated cases in which the adversaries managed to initiate fraudulent message instructions provide interesting data on the beneficiary accounts. SWIFT was able to extract Beneficiary country information from the fraudulent messages sent in 2016 information which revealed some differences in payment techniques. What was most notable, however, was the concentration of the Beneficiary banks in Asia (nearly 89% of all fraudulent transactions had a beneficiary account in East and South East Asia. The remaining 11% was spread over other regions including, in order of magnitude, Europe, North America and the Middle East.

The below graph illustrates the regional location of Beneficiary accounts used in fraudulent transactions since July 2016.



The Payment Controls Service enables banks to implement more effective and robust controls.

Strengthen your defences

The Daily Validation Report tool and Payment Controls Service are part of SWIFT's the state-of-the-art compliance portfolio and an important element in the CBP to strengthen the global financial community's defences against cyber threats as the frequency and speed of payment increases.

Daily Validation Report

The Daily Validation Report tool helps to mitigate the risk of lost records by providing daily activity and risk reporting at your provider's day's SWIFT-based on Activity Reporting allows institutions to verify their payment messages fully against SWIFT's own record – which is critical if customer information is compromised. Risk reporting allows institutions to track on changes in activity that may indicate suspicious activity. Risk profiles aggregated in real-time by country, currency, and flag now correspond to watchlists.

Each day's report covers the previous day's payment activities for MT 103, MT 202, MT 202COV, MT 205 and MT 205COV message types. Reports are delivered via a completely separate, secure on-line channel, direct to compliance and operations teams for monitoring.

Payment Controls Service

The Payment Controls Service enables customers to screen payment instructions safely, before transmission, to detect any lot of unusual message flows.

Using the tool, customers can define their own monitoring policy, controlling their parameters to which they either on and prevention of out-of-policy or unauthorised and therefore potentially high-risk transfer requests.

By understanding the patterns of payments sent over time, the Payment Controls Service enables banks to implement more effective and robust controls. Monitoring rules can also be deployed in real-time to enforce policies and control payment instructions. Doing this reduces the risk of fraud and gives operations teams higher overall control.

Introduction
Targets
Announce
Reconnaissance
Timing
Message Types
Currencies
Beneficiaries
Conclusion

Cyber Security Counterparty Risk Management

In order for customers to assess the level of compliance against the mandatory and advisory controls, SWIFT provides the "Know Your Customer – Security Assessment Tool" as the central application for the suppression of red indicator codes. The KYC-SAC application also enables each customer to facilitate the transparent exchange of their security status information with their counterparties to support cyber risk management and business due diligence.

The transparency provided by this counterparty data exchange system is driving adoption and compliance with the controls, as institutions seek to demonstrate their cyber security to their counterparties.

Cyber security risk introduced by counterparty risks is so managed across different types of risk. Many institutions are therefore already integrating cyber risk assessments into their existing risk processes by incorporating the counterparty risk assessment (CSCA) at the on data into their risk management and business conduct-making processes.

As outlined in the recently published guidance "Managing Cyber Security Counterparty Risk – A Getting Started Guide", institutions can assess the cyber security risk posed by their counterparties by:

- Collecting the necessary data and controlling how it is used to support decision-making.
- Processing this data and transforming it into a structured risk-based assessment, typically shared with teams to ensure a risk-based approach is used.
- Adopting suitable countermeasures to mitigate or "treat" the risk.

To support the risk assessment of incoming transactions from counterparty entities, institutions should assess how incoming transactions from counterparties compare against the profile of existing incidents, e.g. country/region of sending counterparty, contribution of and sensitivity, transaction type, transaction currency, transfer or value, transfer or timing and country.

These parameters are described in the Getting Started Guide and should be used by institutions to assess levels of counterparty risk.

Conclusion

The global financial community has seen a continued evolution in the cyber threat since 2016, with financial institutions facing attacks of increasing levels of sophistication.

In responding to this challenge, SWIFT will continue to promote robust cyber security standards, new security standards and services, and work to increase the scope and quality of threat intelligence sharing.

Our information sharing initiative has continued to support the improvements in the community's collective cyber defences as well as the introduction of fraud detection and prevention capabilities, such as the **Payment Controls Service** and the **Daily Validation Report** tool. These products are aimed at mitigating the risks associated with cyber fraud and are designed to support the financial community's broader initiative to secure already existing in place.

The industry should continuously increase the strength and diversity of its defences and ensure it now understands the nature of the changing threat. This means being proactive in identifying and applying the best practices, and business practices, means creating robust processes and understanding counterparty cyber risk.

Cyber security risk introduced by counterparties needs to be managed alongside other types of risk.

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

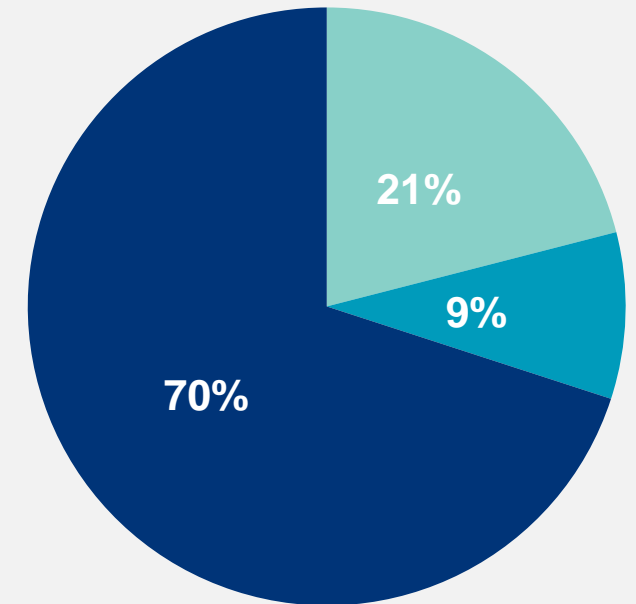
During the most recent investigations, the number of fraudulent transactions issued averaged around ten per incident within a two-hour period



Key Takeaways

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



■ EUR ■ Other ■ USD



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

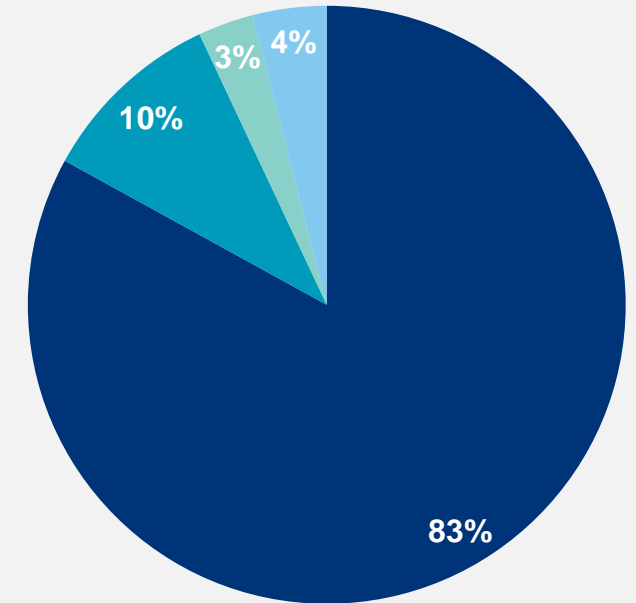
Most of the transactions issued were handled by one or two Receiver banks and were intended for the same Beneficiary country

Key Takeaways

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.



■ Asia Pacific ■ Europe
■ Middle East ■ North America



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



Cyber attackers

Compromise institution's environment

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



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



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



Cyber attackers

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

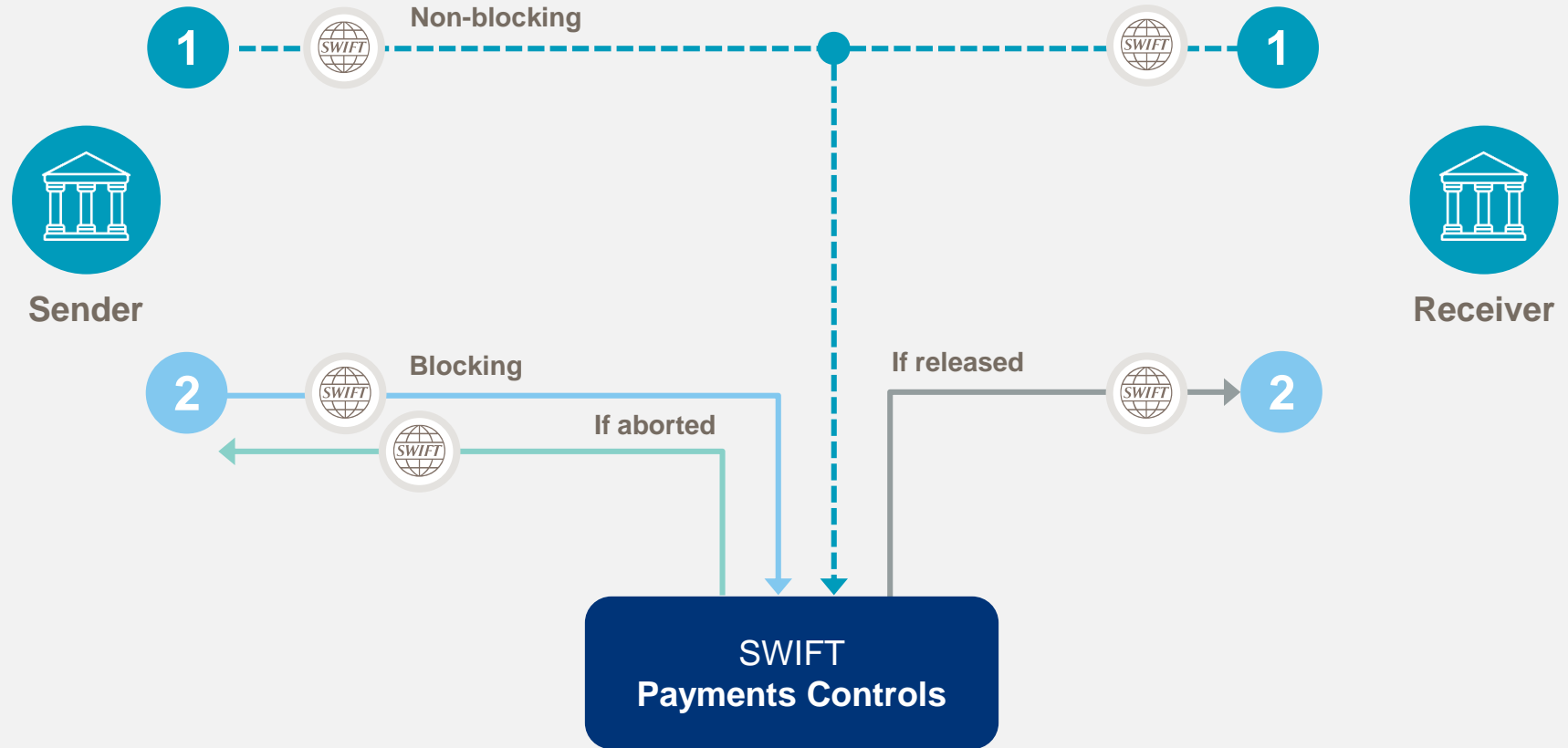


What are the benefits of Payment Controls?

- 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

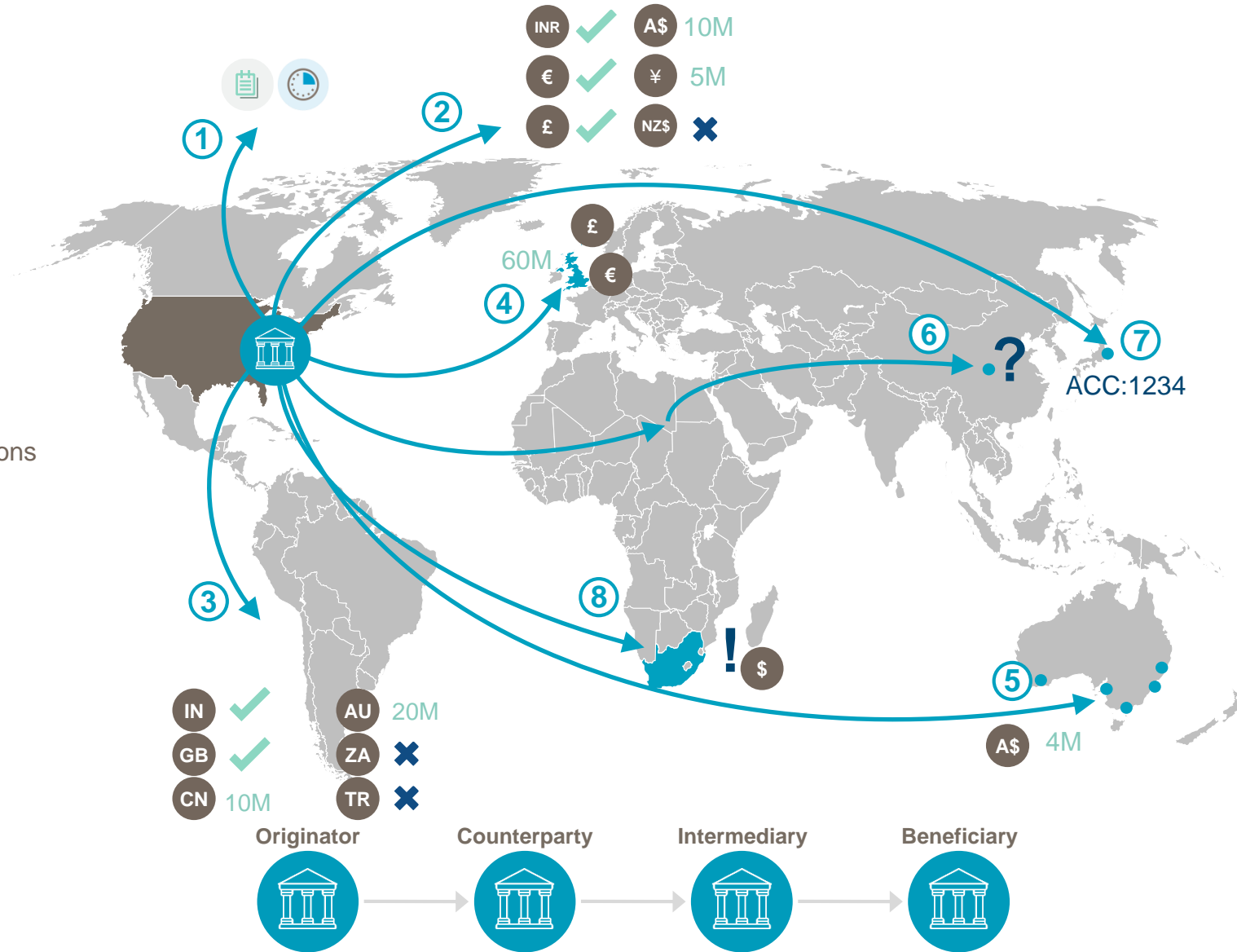


A few examples...

Flexible parameters including:

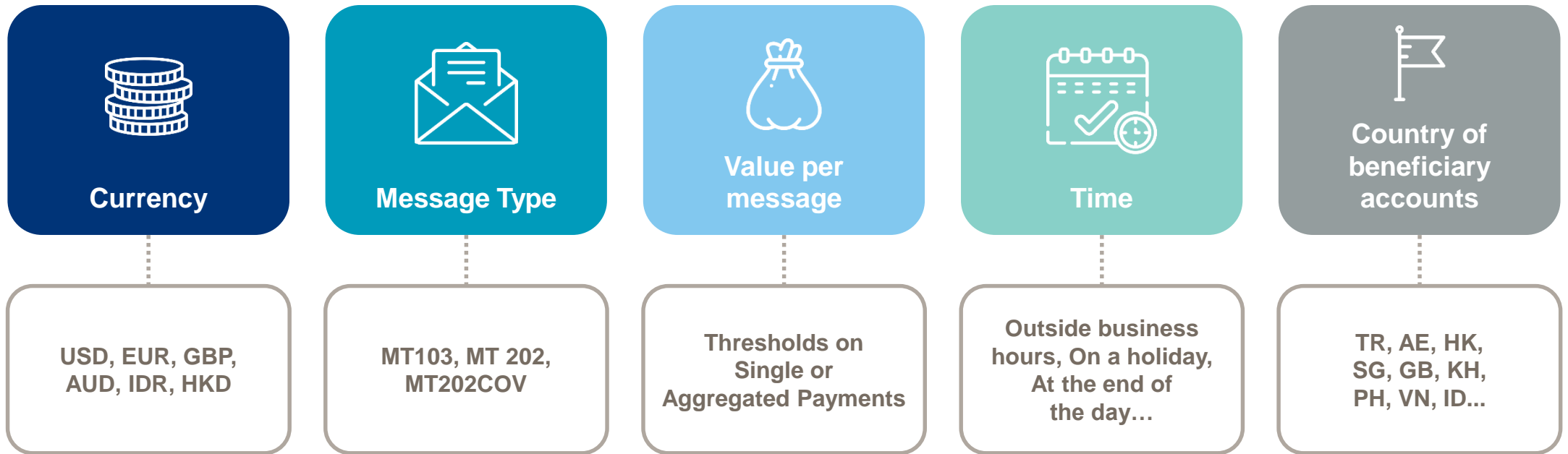
- ① Business hours and days
- ② Currency whitelist / blacklists, single & aggregate payment limits
- ③ Country whitelist / blacklists, single & aggregate payment limits
- ④ Country & currency threshold combinations
- ⑤ BIC & Entity institution limits
- ⑥ New payment flows
- ⑦ Suspicious accounts
- ⑧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