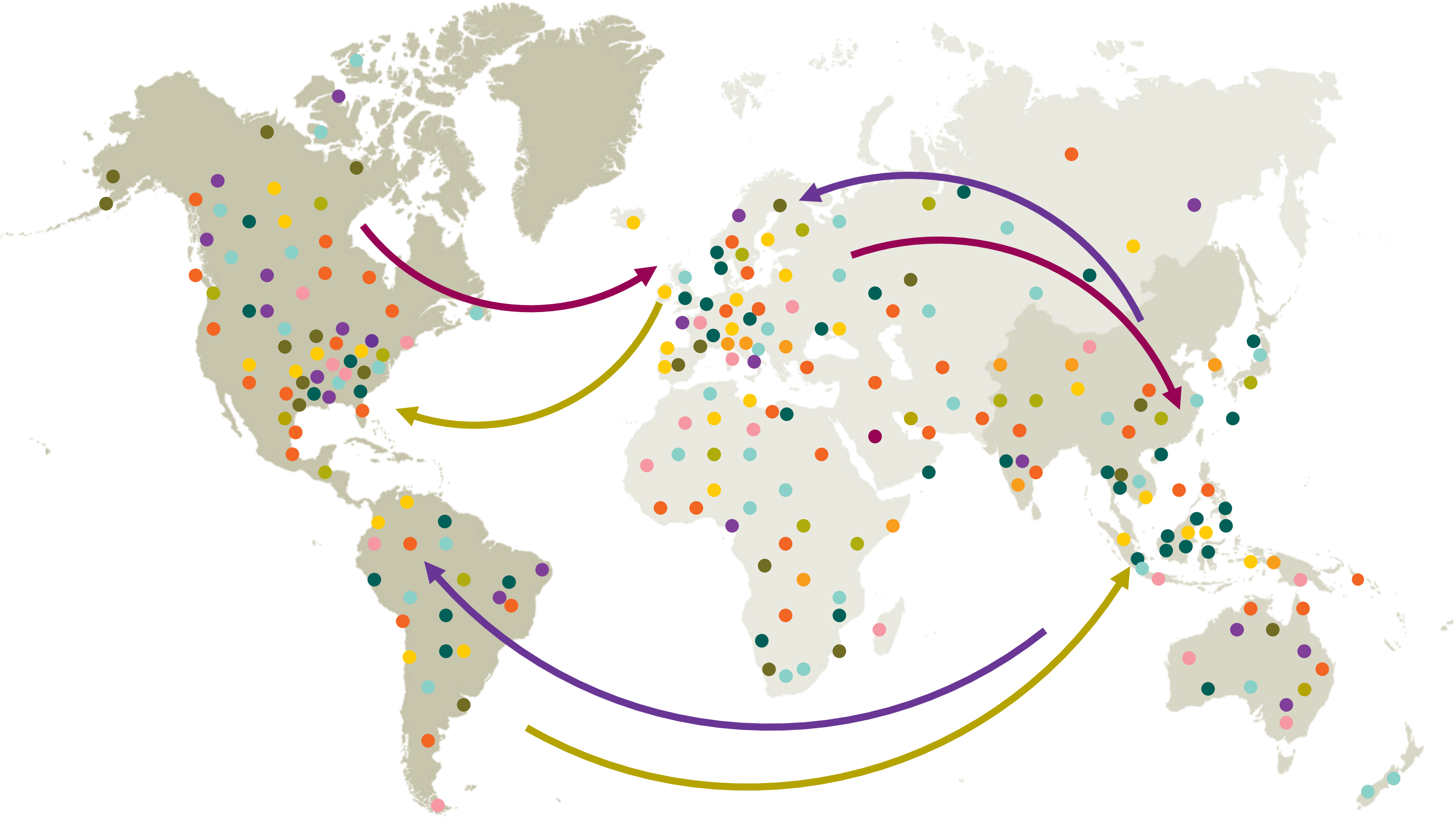
SWIFT Webinar:
Protect your institution against payment fraud

Thomas Preston

7 February 2019

SWIFT is a global provider of secure financial messaging services

Industry owned, financial services cooperative, that does not seek to maximise profit



Connecting
12,000+
institutions

200+
Countries
and territories

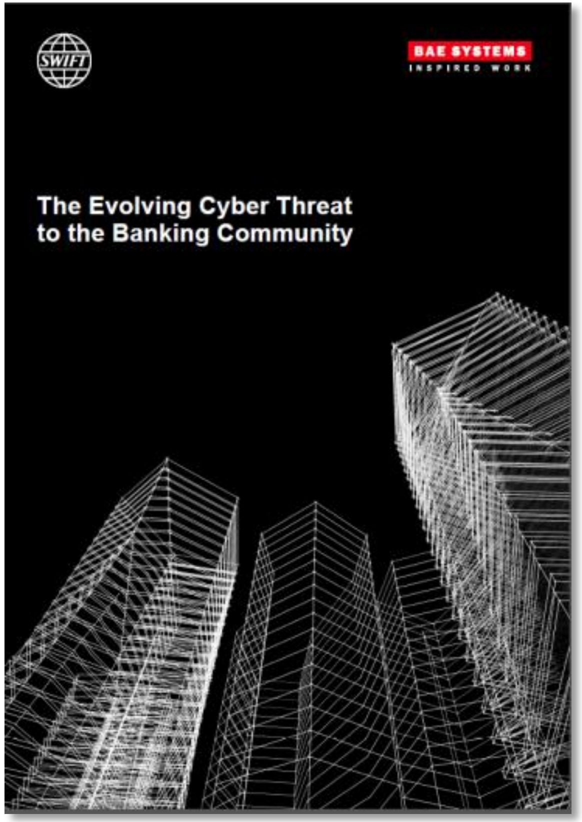
7+ billion
FIN messages
in 2017

Proven network **99.999%**
FIN availability

Strong PKI
security
encryption

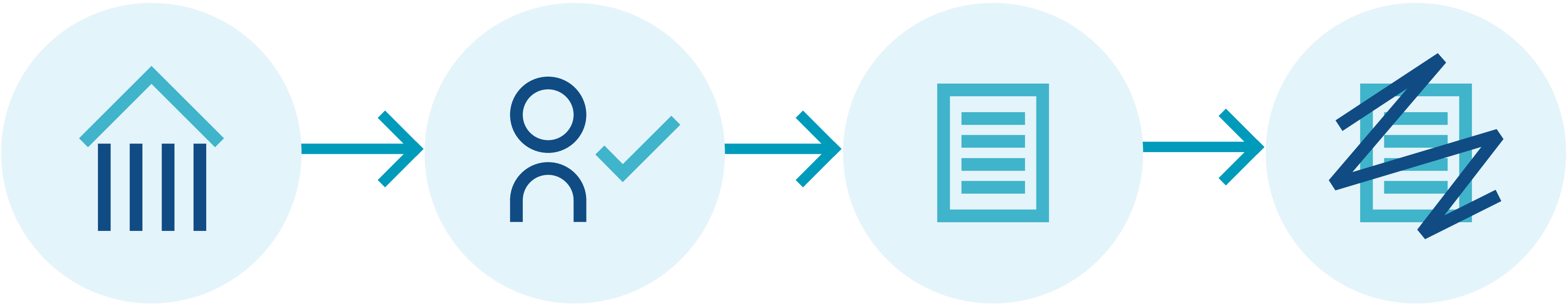
ISO 20022
Unique role
developing
standards

Attacks on SWIFT members have the same modus operandi



The Evolving Cyber Threat
to the Banking Community

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

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

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

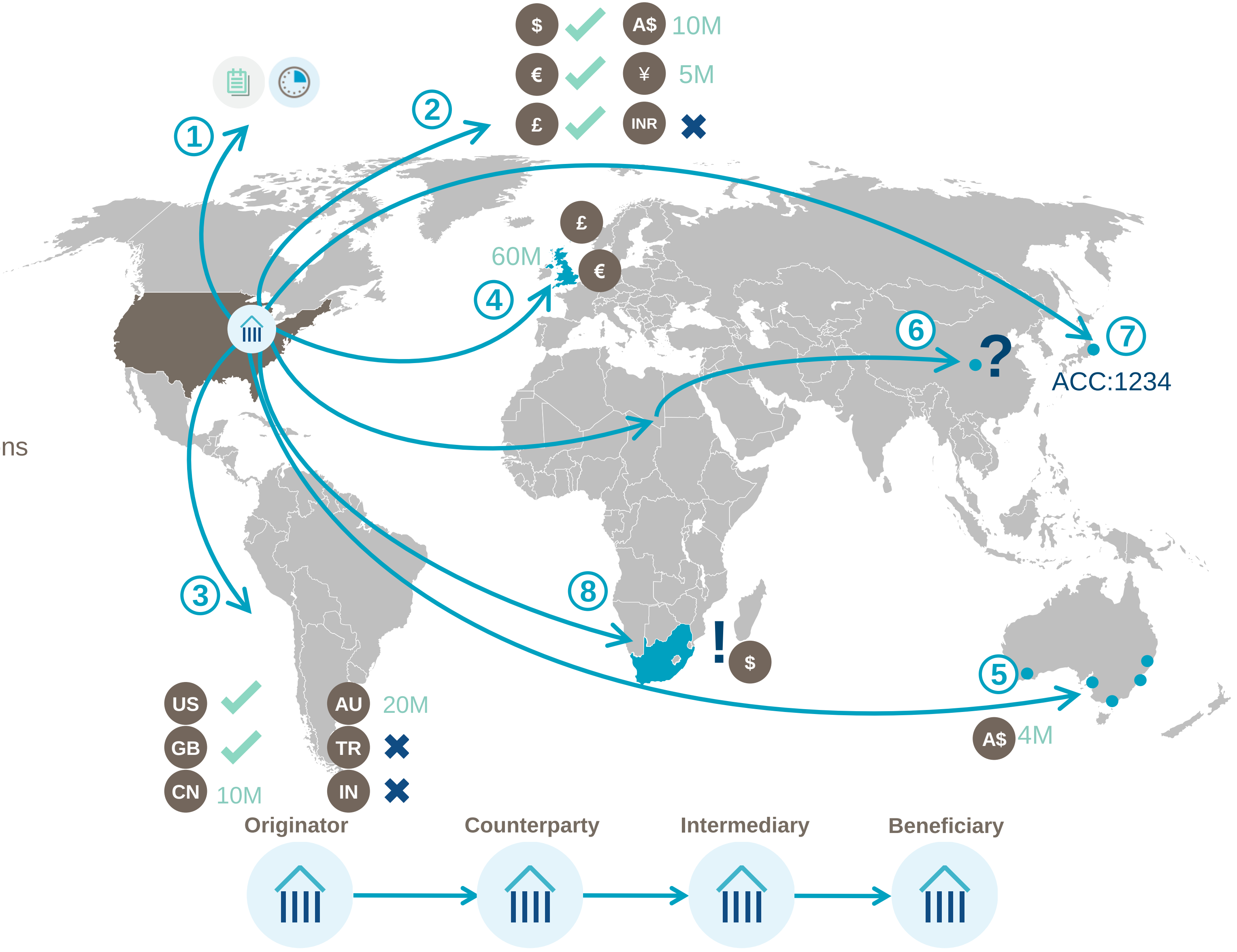
⑤ BIC & Entity institution limits

⑥ New payment flows

⑦ Suspicious accounts

⑧ Uncharacteristic behaviours

+ Across the complete payment chain



reduce
fraud risks

reduce
reputational
risks

build
trust

www.swift.com