СВИФТ и кибербезопасность
Текущий статус
SWIFT and Cybersecurity
An update

IXth Ural Finance Information Security Forum
14-Feb-2018

Матвей Геринг / *Matthieu de Heering*
Head of Central and Eastern Europe
SWIFT

Agenda

1 SWIFT Customer Security Programme (CSP) update

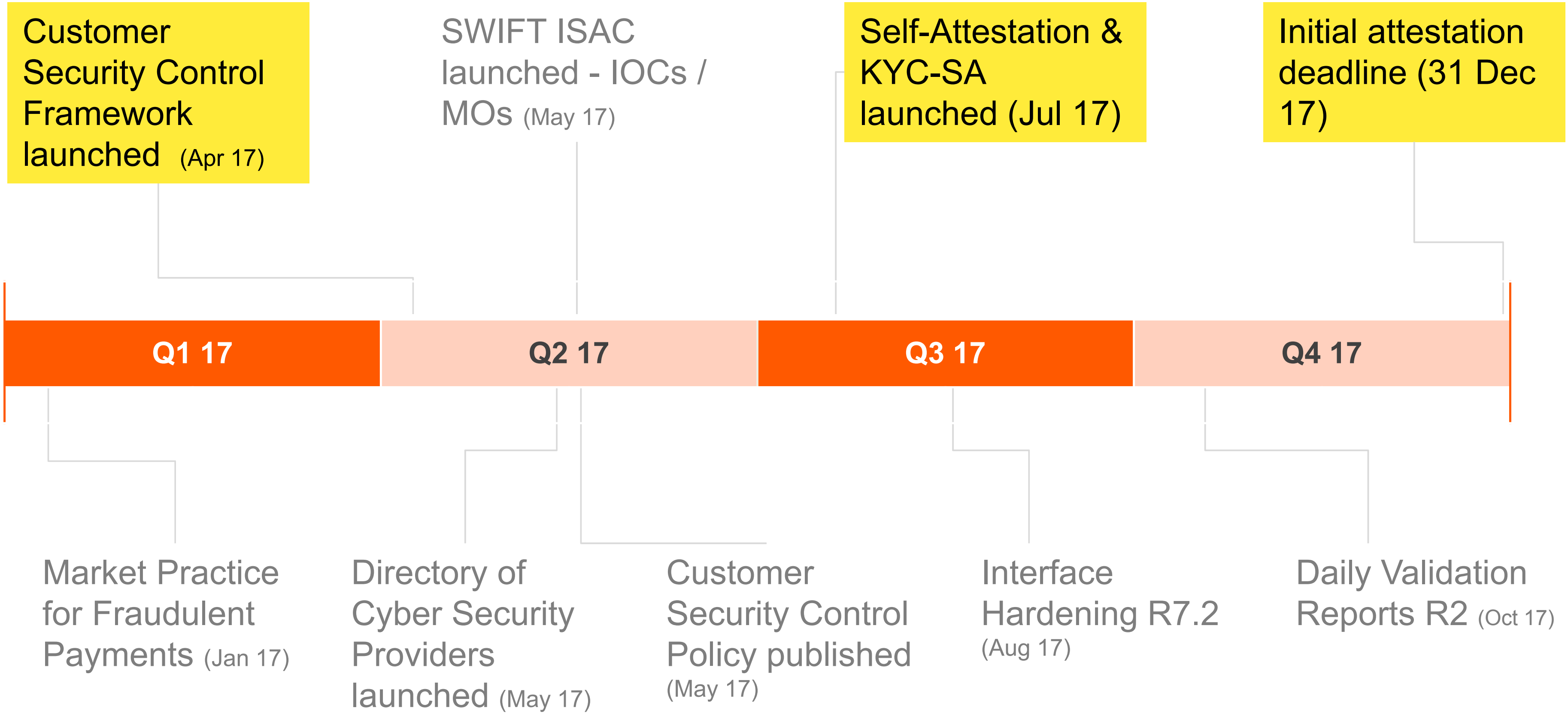
2 Evolution of cyber-threats to the global banking community

3 SWIFT’s anti-fraud tools - focus on Payment Controls & Daily Validation Reports

Customer Security Programme

Brief update

CSP update | 2017 milestones



Customer Security Control Framework launched (Apr 17)

SWIFT ISAC launched - IOCs / MOs (May 17)

Self-Attestation & KYC-SA launched (Jul 17)

Initial attestation deadline (31 Dec 17)

Q1 17

Q2 17

Q3 17

Q4 17

Market Practice for Fraudulent Payments (Jan 17)

Directory of Cyber Security Providers launched (May 17)

Customer Security Control Policy published (May 17)

Interface Hardening R7.2 (Aug 17)

Daily Validation Reports R2 (Oct 17)

CSP update | Attestation

89% of customers attested their level of compliance with the mandatory controls by the 31 December 2017 deadline

This was an overwhelmingly positive response from the community – across every segment, market and infrastructure type.

All customers now need to self-attest that they fully comply with all mandatory security controls by 31 December 2018.

Self-attestations need to be renewed every 12 months.

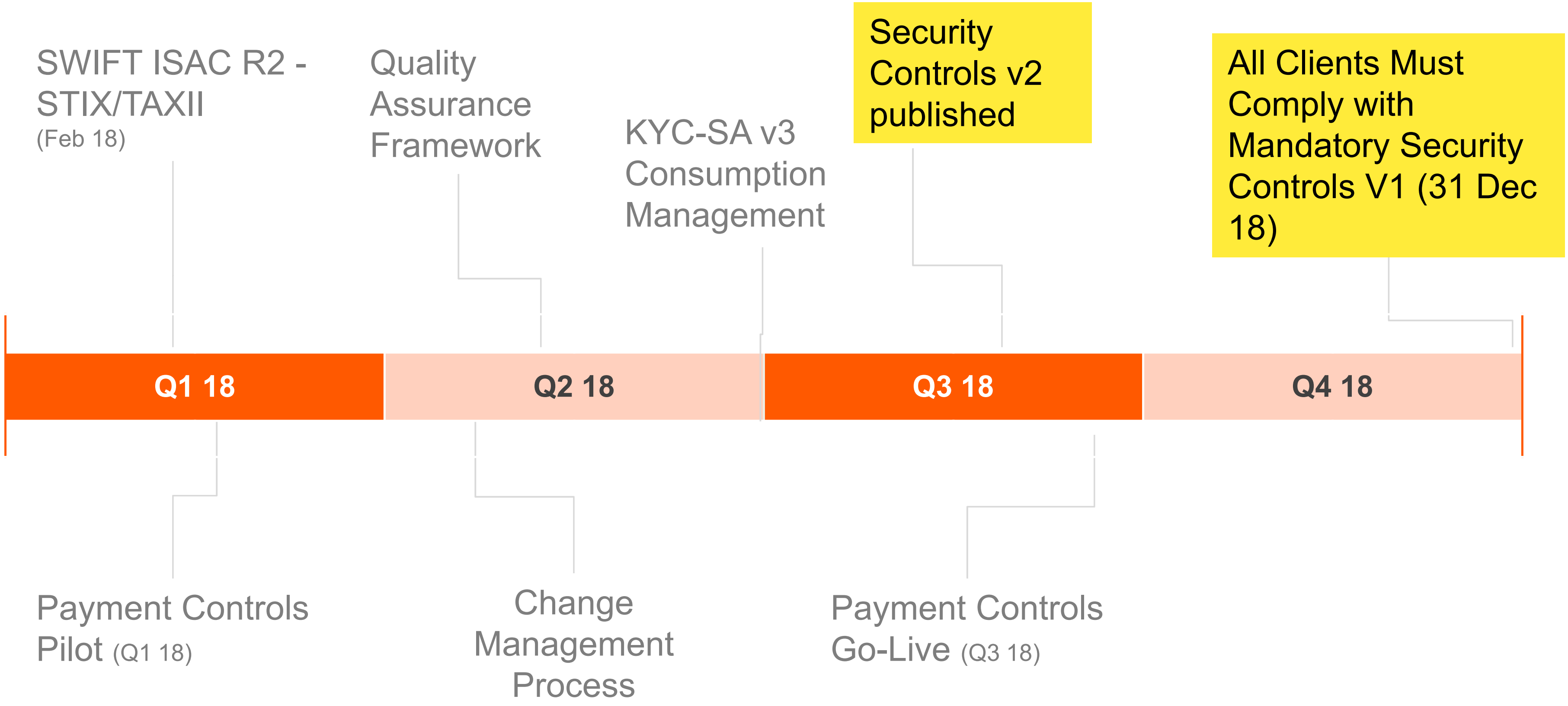
89%

BICs globally that self-attested by the deadline

99%

Attested BICs represent 99% of the FIN Traffic

CSP update | 2018 deliverables



SWIFT ISAC R2 - STIX/TAXII (Feb 18)

Quality Assurance Framework

KYC-SA v3 Consumption Management

Security Controls v2 published

All Clients Must Comply with Mandatory Security Controls V1 (31 Dec 18)

Q1 18

Q2 18

Q3 18

Q4 18

Payment Controls Pilot (Q1 18)

Change Management Process

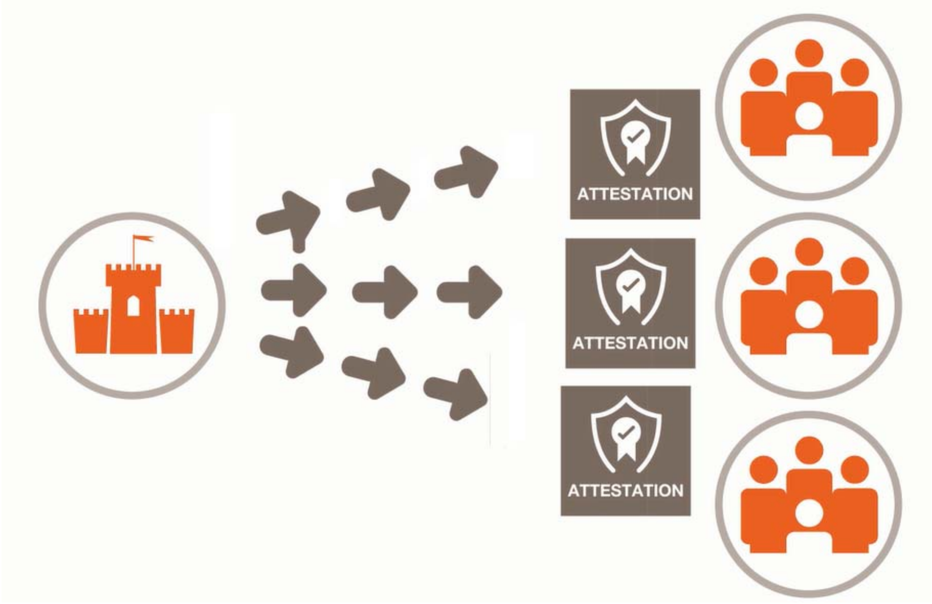
Payment Controls Go-Live (Q3 18)

CSP update | Consumption

Users should consume counterparty attestation data and integrate this into their risk management and business decision-making processes.

Using the KYC-SA, customers can share their attestation data with their counterparties and request data from others.

Customers remain in control of their attestation data – they can grant or deny requests of their attestation data.



Actions customers can take

CSP Update | What you can continue to do

1. Engage in SWIFT ISAC and sign up for notifications.

2. Ensure mandatory security updates of SWIFT software are installed.

3. Ensure that you fully comply with all the mandatory security controls and attest by 31 December 2018.

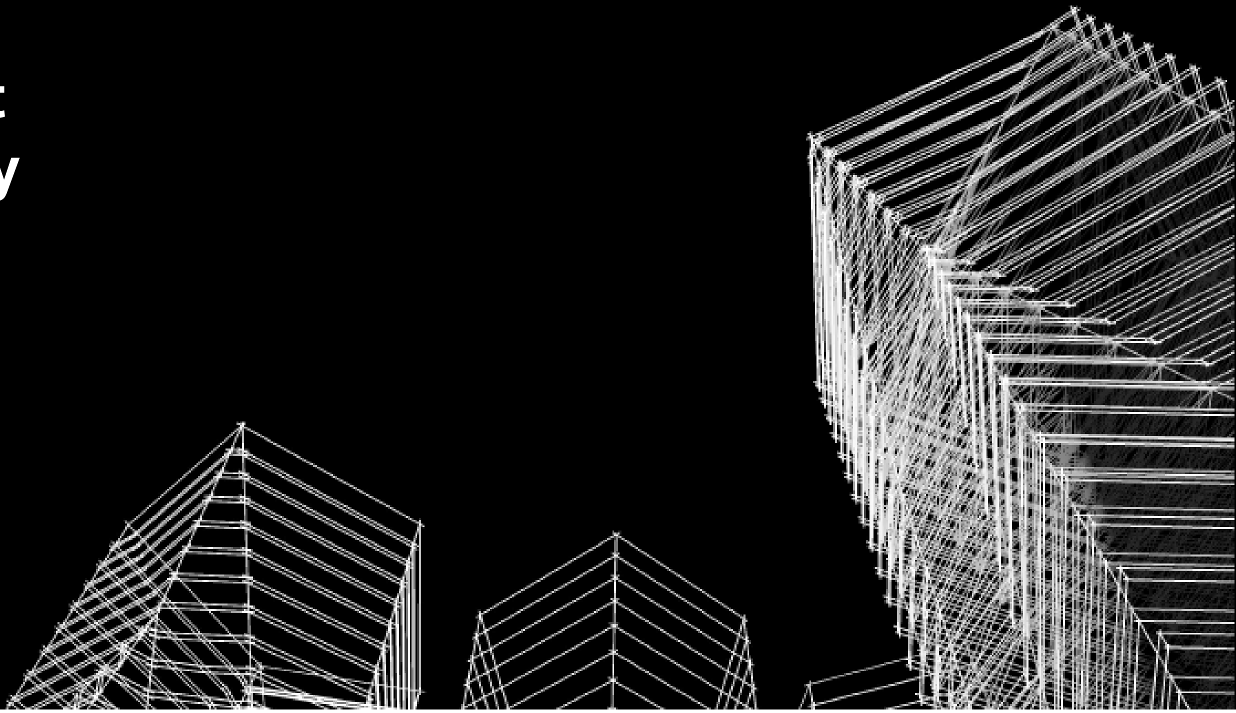
4. Consider your institution’s counterparty risk frameworks to consume and utilise counterparty attestation data.

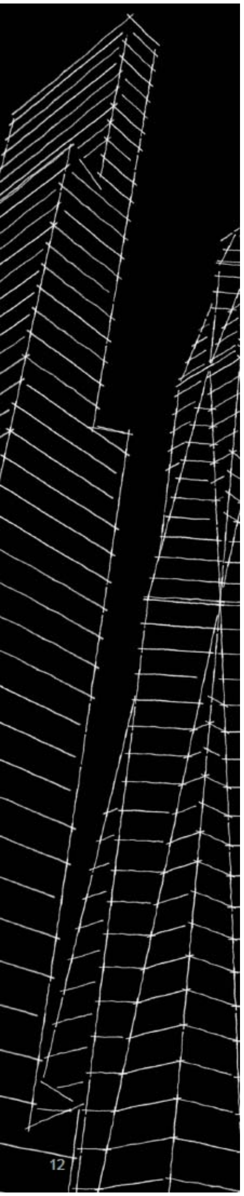
5. Consider SWIFT’s anti-fraud tools (Payment Controls, Daily Validation Reports, RMA clean-ups, etc.)

SWIFT

BAE SYSTEMS
INSPIRED WORK

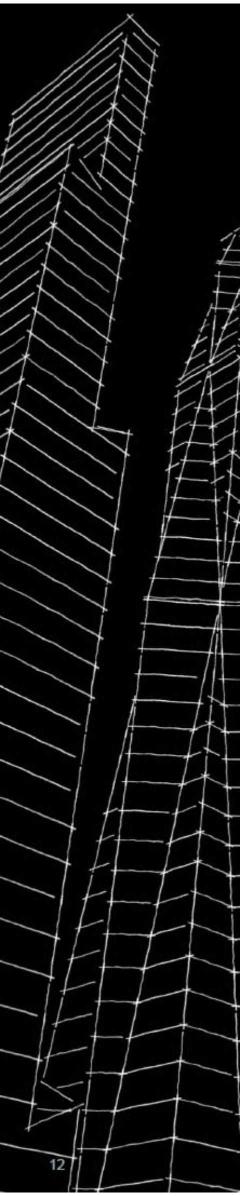
The Evolving Cyber Threat To the Banking Community





Background

- The February 2016 attack was a watershed moment for the payments industry. Though not the first case of fraud against a bank’s payment endpoint, it was the scale and sophistication of the attack which shook the global community
- The attackers not only had a detailed knowledge of the business processes involved in interbank payment messaging, but also reverse-engineered the specific interface software running at the victim bank
- With this knowledge they built custom malware both to aid sending fraudulent messages and to cover-up the evidence to enable their getaway. This was highly coordinated and took advantage of a local public holiday
- Other cases occurred as other attackers ramped up copy-cat attacks
- Software updates were released to mitigate specific attack vectors, e.g. improved database integrity checks, but the attackers continued their reverse-engineering efforts and updated their malware too
- In all cases, security weaknesses in the victim banks led to the attackers’ gaining Administrator access. With this they could monitor the banks’ operations, modify victims’ security defences, update firewall rules, and bypass security features



Evolving Attack Techniques

Protection

- Attackers protect their malware from being analysed and their secrets revealed
- Attackers sometimes rely on commercial protector products – Enigma and VMProtect
- Protection is notoriously difficult to break

Stealthiness

- Attackers use fileless modules that were loaded into memory from the registry
- When files are written to the hard drive, they are encrypted and camouflaged to blend with other legitimate system files

Wipe-Out Techniques

- Attackers employ anti-forensic techniques to erase traces of their own activity making retracing and understanding their actions difficult
- Subsequent investigators may not find any digital fingerprints

Highjacking

- Attackers hijack legitimate software to manipulate its logic or monitor in-transit data
- One malicious module was re-programmed to always return “success” result, even if the software attempted to throw an alert

Surveillance

- Attackers deploy malicious modules that takes screen shots and records keystrokes
- Screenshots were encoded into a video format, allowing the attackers to ‘watch’ and understand the business processes. This surveillance can take many months

False-Flags

- Attacker place ‘false-flags’ in their malware, depicting (fictitious) tell-tale signs and patterns, e.g. false language codes or incorrectly transliterated words
- False-flags are an attempt to put investigators off the tracks

Anonymity

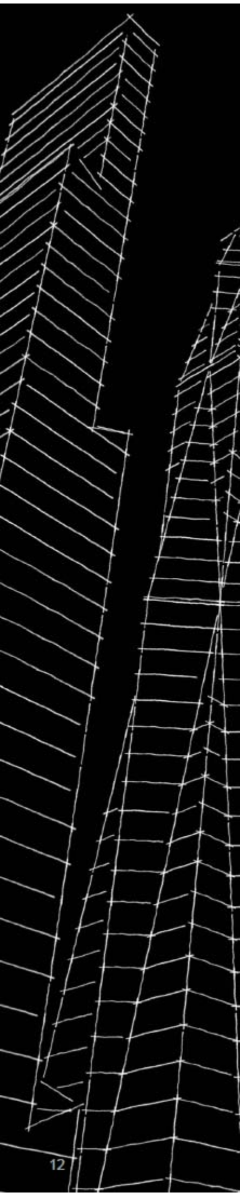
- Attackers set up a number proxy hops between themselves and the end-target
- This long chain of events is difficult for investigators to understand and trace. If the number of such proxy hops is > 3, it is very difficult to establish the real attacker

Watering Holes

- In order to target victims, the attackers may not want to engage with them directly
- Attackers ‘bait’ a legitimate web site and patiently wait for the victim to visit
- If the visitor is of interest, then they attempt to infect the victim’s machine

Exploits

- Attackers search for ‘holes’ in systems. Once found, they penetrate and compromise nodes, one after another
- Attackers only needs to find one hole, but the defender needs to fix all holes



Basic Defences and Counter-Measures

Secure your Environment

- Deploy a layered security architecture, across physical and logical
- Prevent and detect, segregate and isolate
- use Anti Virus tools and keep all software up to date

Know and Limit Access

- Limit and protect administrator and system privileges
- Employ strong ID management with roles, profiles and password rules
- Use multifactor authentication

Detect and Respond

- Deploy intrusion detection capabilities, with triggers and tripwires
- Monitor alerts for suspicious activity
- Monitor unusual behaviour, e.g. out of hours, new systems, multiple failed passwords

Threat Intelligence

- Know your adversary
- Share and consume information
- Act on recommendations

Limit Exposures

- Only do business with trusted counterparties
- Actively maintain your RMA relationships
- Remove non-current relationships

Security Controls

- Implement the security controls
- Complete self-attestation by end Dec 17
- Ensure compliance with all mandatory controls by Dec 18

Know Your Counterparties

- From Jan 18, request your counterparty's self-attestation against the security controls
- Assess their risk, based on the KYC-SA profile
- Put in place relevant controls calibrated to the perceived cyber-risk

Other Business Controls

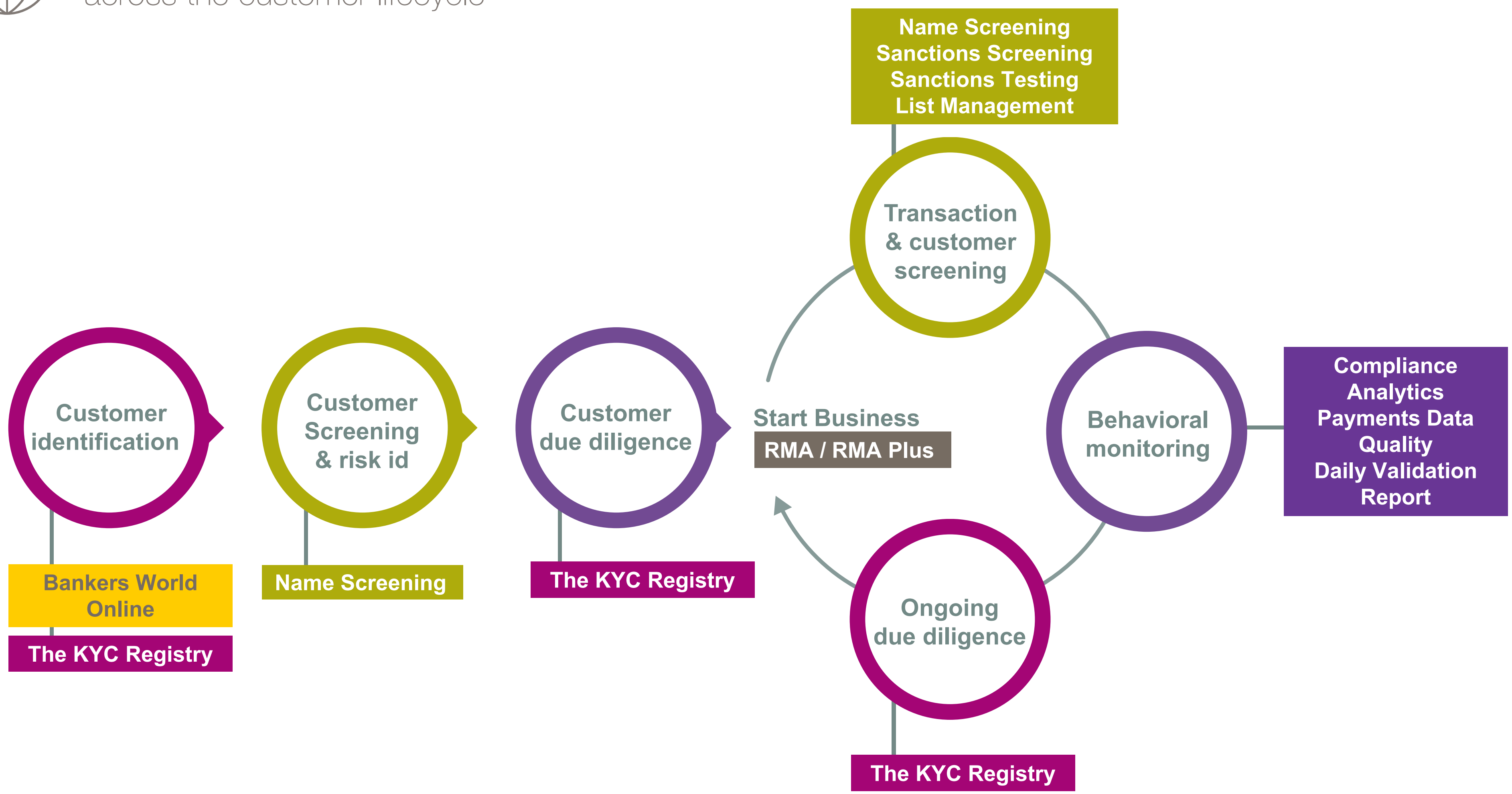
- Screen your outgoing payments to detect illicit or unusual message flows
- Take immediate remedial action for out-of-policy messages
- Reconcile against confirmation and statement messages

Incident Response

- Institute and practice response and recovery - it raises the chances of funds recovery
- Know how to send a cancellation message, if you suspect fraud
- Know what to do with a cancellation message, if you receive one

Financial crime compliance services

across the customer lifecycle



Customer identification

Bankers World Online

The KYC Registry

Customer Screening & risk id

Name Screening

Customer due diligence

The KYC Registry

Start Business

RMA / RMA Plus

Transaction & customer screening

Name Screening
Sanctions Screening
Sanctions Testing
List Management

Behavioral monitoring

Compliance Analytics
Payments Data Quality
Daily Validation Report

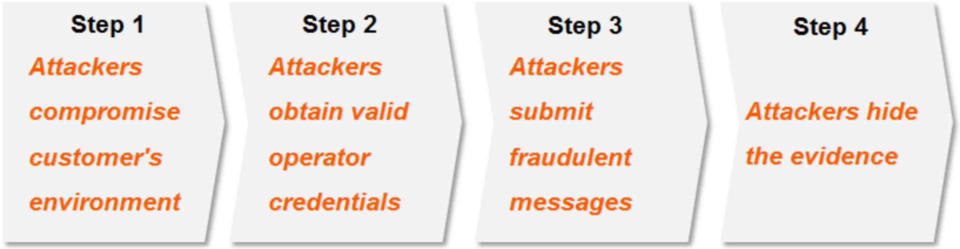
Ongoing due diligence

The KYC Registry

CSP & Transaction Pattern Detection

- *Daily Validation Reports*
- *Payment Controls Service*

Daily Validation Reports – responding to the insider threat



Step 1 *Attackers compromise customer's environment*

Step 2 *Attackers obtain valid operator credentials*

Step 3 *Attackers submit fraudulent messages*

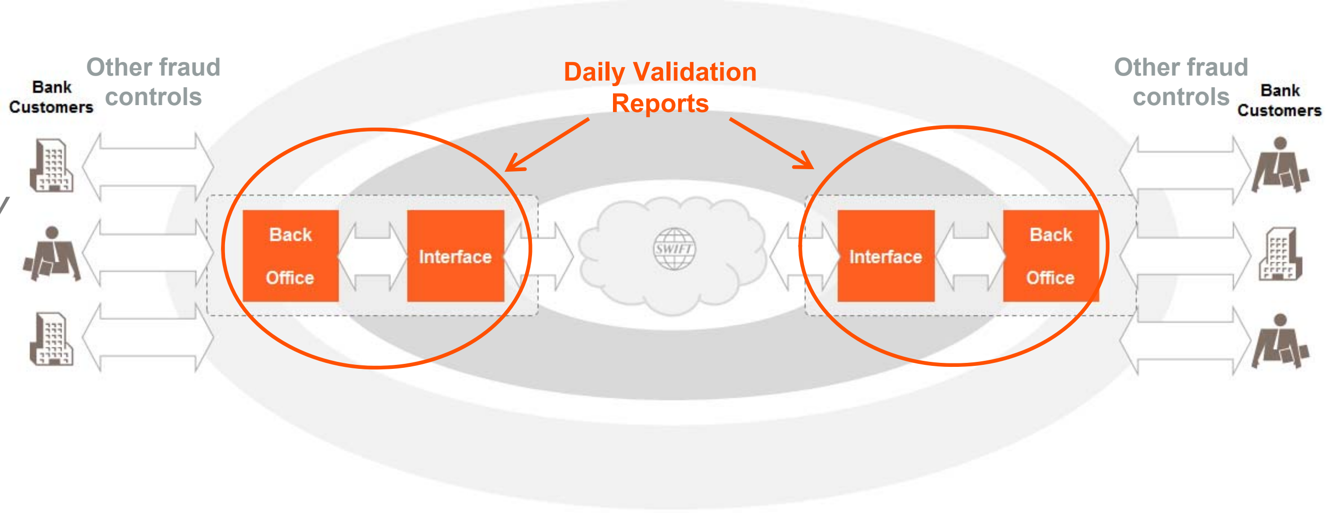
Step 4 *Attackers hide the evidence*

Attackers are organised, sophisticated and well funded

➔ **In the event of an attack, accuracy of data in interface systems may be compromised**

Banks need to verify the integrity of payments across ***back-office*** and interface systems

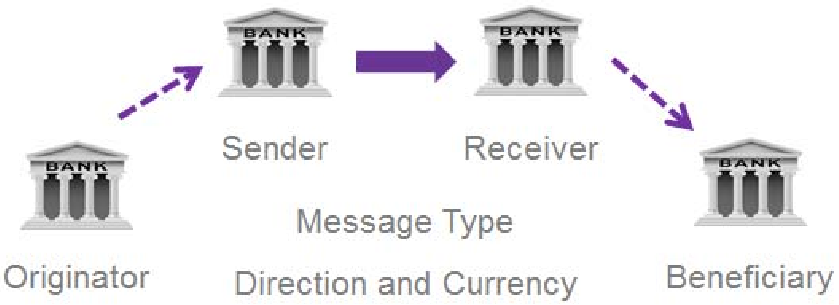
Daily Validation Reports - *provide a way to access SWIFT's record of transaction activity to mitigate this insider threat and not having to rely on, possibly compromised, interface systems.*

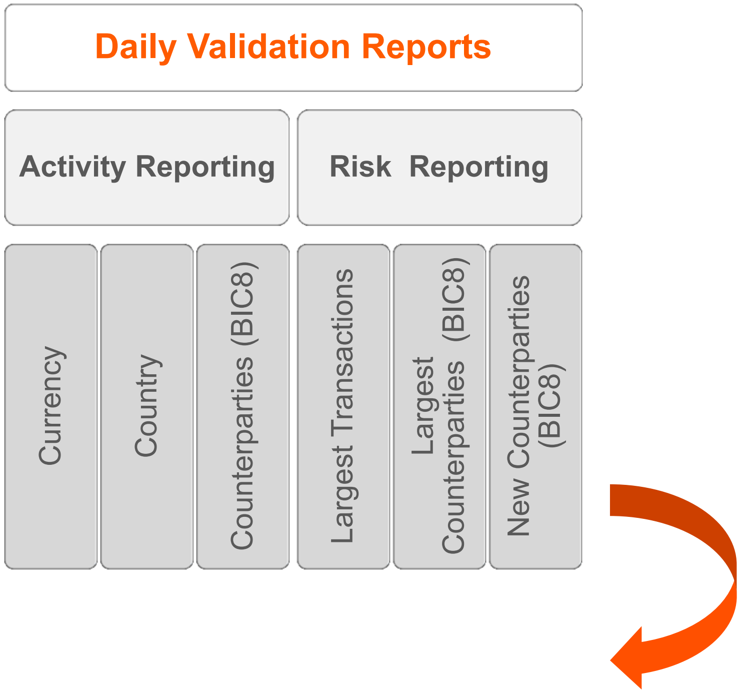


Daily Validation Reports

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





Daily Validation Reports

Activity Reporting

Risk Reporting

Currency

Country

Counterparties (BIC8)

Largest Transactions

Largest Counterparties (BIC8)

New Counterparties (BIC8)

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

How Daily Validation Reports can help identify fraud – A fictitious scenario

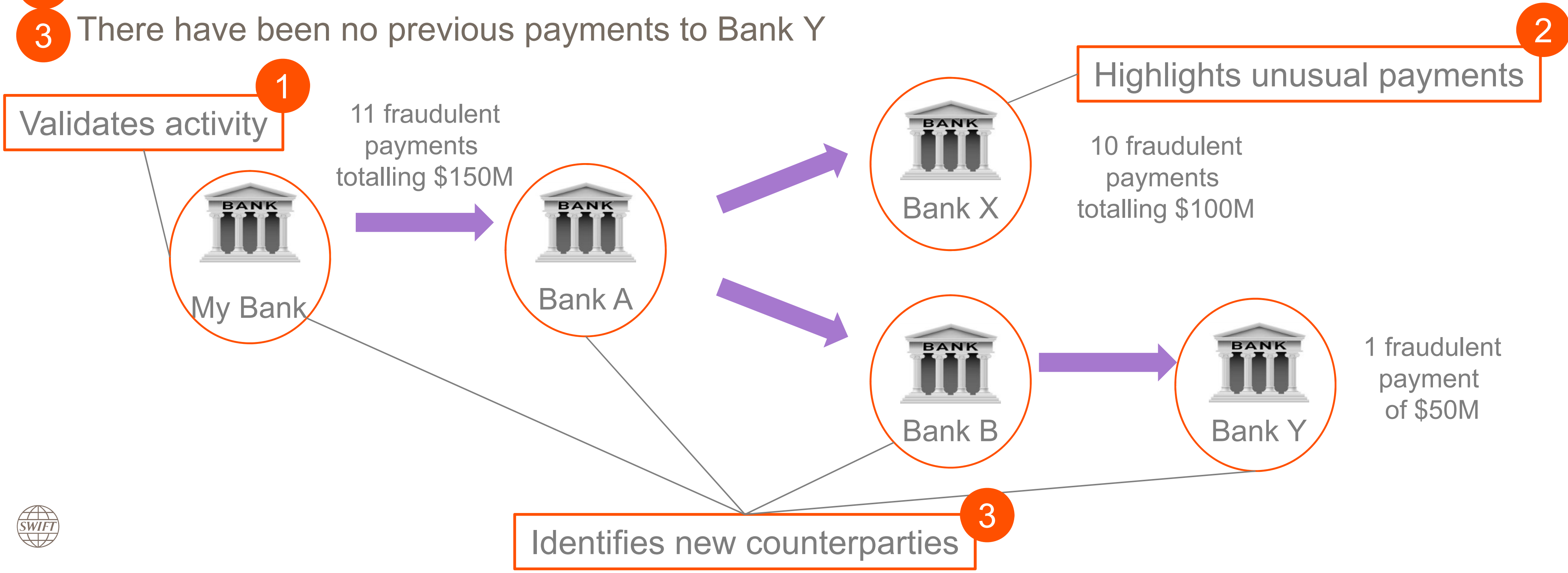
Attackers gain access to the back office systems of “My Bank” and send fraudulent payments.

A total of $150M in fraud is sent from “My Bank” to accounts in Bank X ($100M) and Bank Y ($50M).

1 Statements are intercepted by malware in My Bank’s environment – payment records are wrong!

2 Payments to Bank X are uncharacteristic, values are usually lower!

3 There have been no previous payments to Bank Y



1 Validates activity

11 fraudulent payments totalling $150M

2 Highlights unusual payments

10 fraudulent payments totalling $100M

1 fraudulent payment of $50M

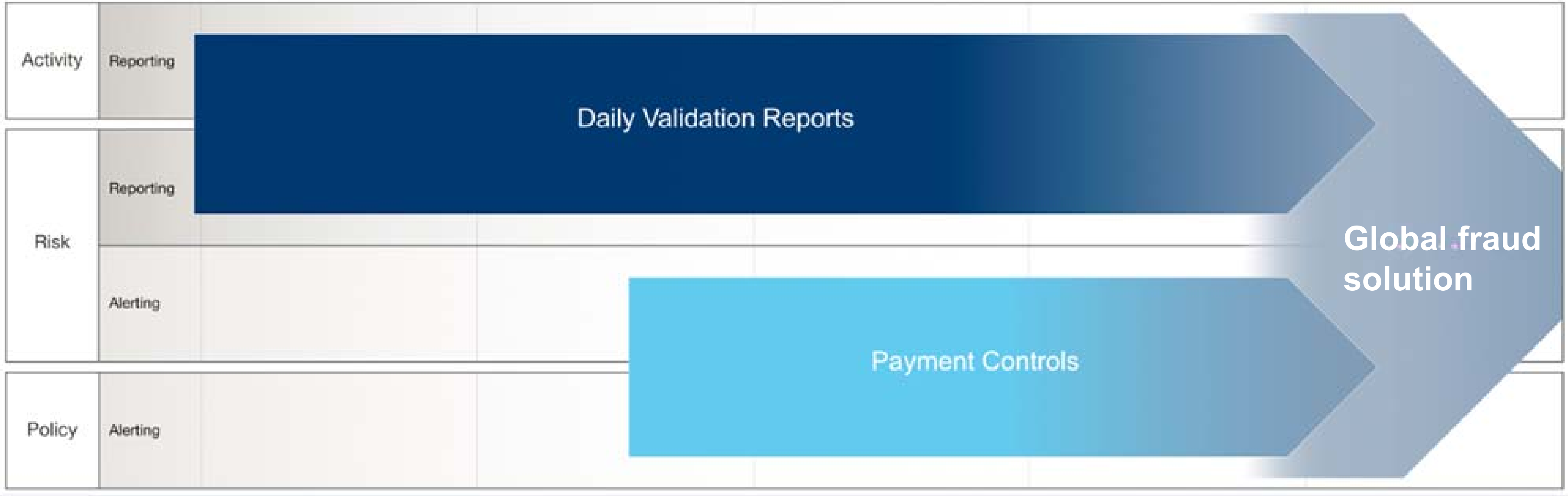
3 Identifies new counterparties

Fraud Prevention Roadmap | A complete fraud prevention solution

In your strategy to protect yourself against cyber-threat:

- **Do you report on your activity on a daily basis?**
  - Are you confident that your reporting is not compromised?
  - Do you look back in time to understand normality of activity?
- **Have you defined a risk policy/ a payments policy**
  - Can you ensure their enforcement?
  - Identify in real time non compliant payments?

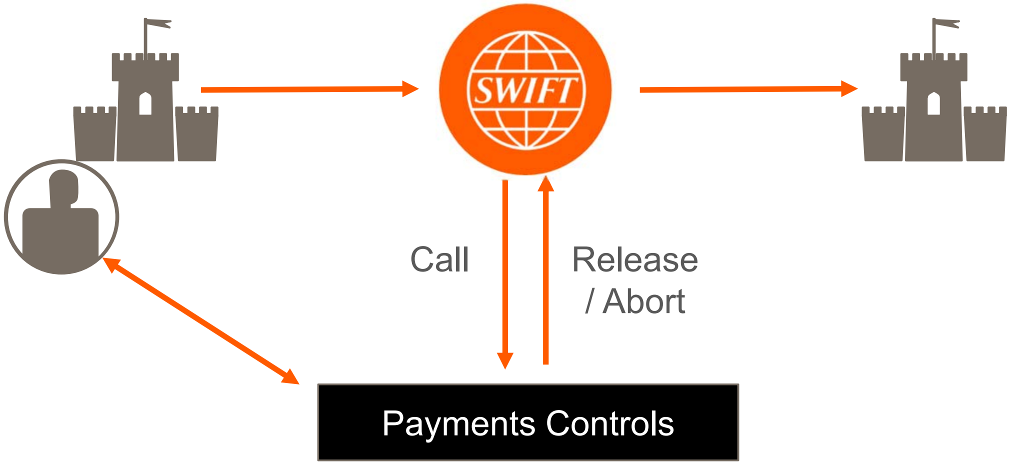
Roadmap



Services as safeguards to help address, as part of other controls, the mandatory Logging and Monitoring requirements (section 6.4) and the Transaction Business Control requirements (section 2.9)

Payment Controls | **Capabilities**

Q3 2018



Key CSP deliverable that:

- Protects **outbound payments** of smaller banks
- Reduces **inbound risk** for larger correspondents

Secure in-network, real-time monitoring:

- Independent of back-office
- Zero footprint (secure token access)
- Blocking and non-blocking modes (SSS model)
- Customer sets and controls monitoring policy
- Standard alert review workflows / escalation paths
- Baseline ruleset developed with our community
- Full audit trail for monitoring policy management and alert investigation
- MT101, MT103(+), MT202(COV) and MT205(COV)*

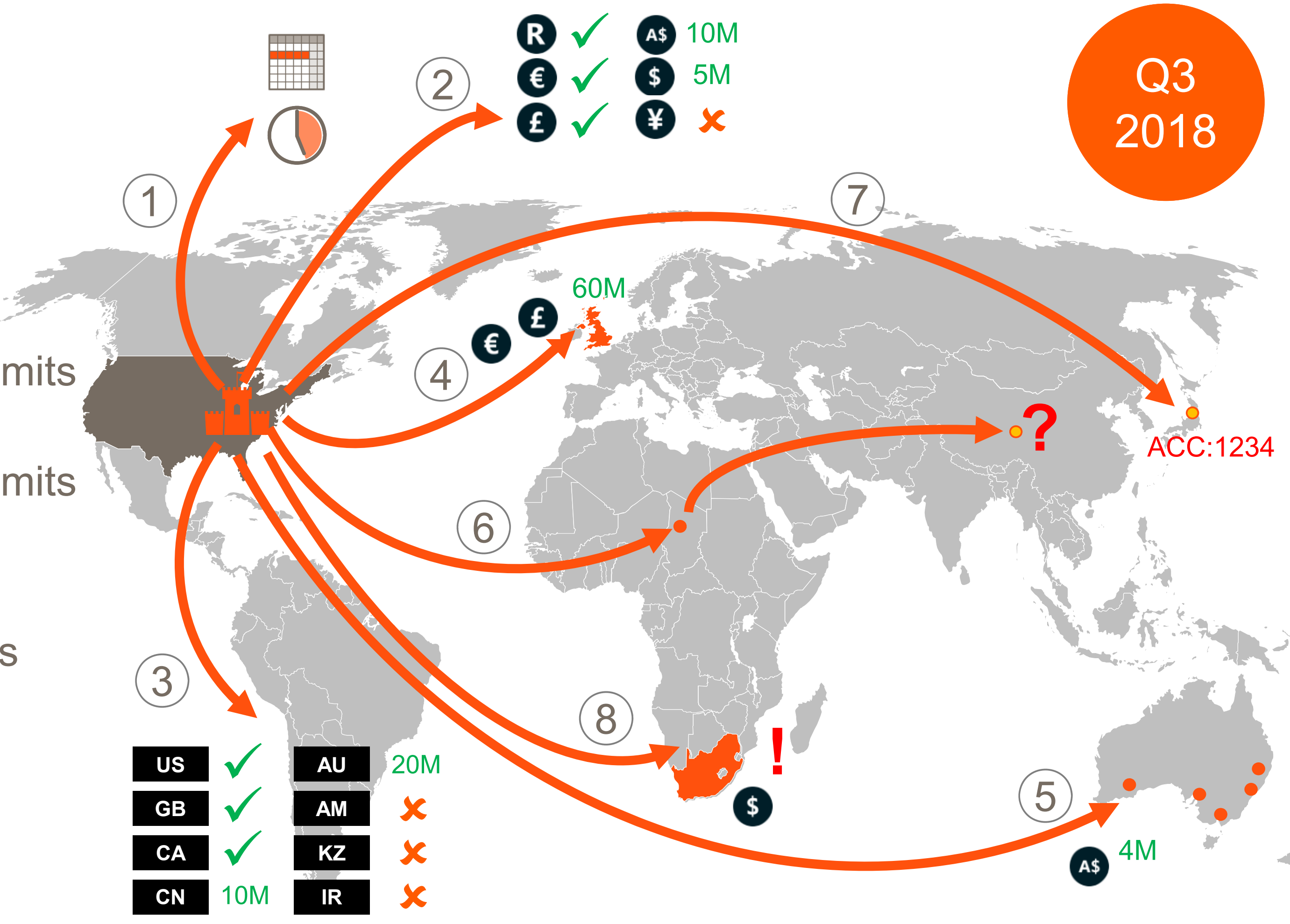
*Additional message types, including MX, are under consideration

Payment Controls | **Capabilities**

Flexible parameters including:

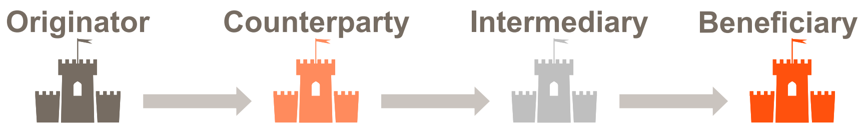
1. Business hours and days
2. Currency whitelist / blacklists, single & aggregate payment limits
3. Country whitelist / blacklists, single & aggregate payment limits
4. Country & currency threshold combinations
5. Single & group institution limits
6. New payment flows
7. Suspicious accounts
8. Uncharacteristic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

Across the complete payment chain



R	✓	A$	10M
€	✓	$	5M
£	✓	¥	✗

US	✓	AU	20M
GB	✓	AM	✗
CA	✓	KZ	✗
CN	10M	IR	✗



SWIFT

www.swift.com