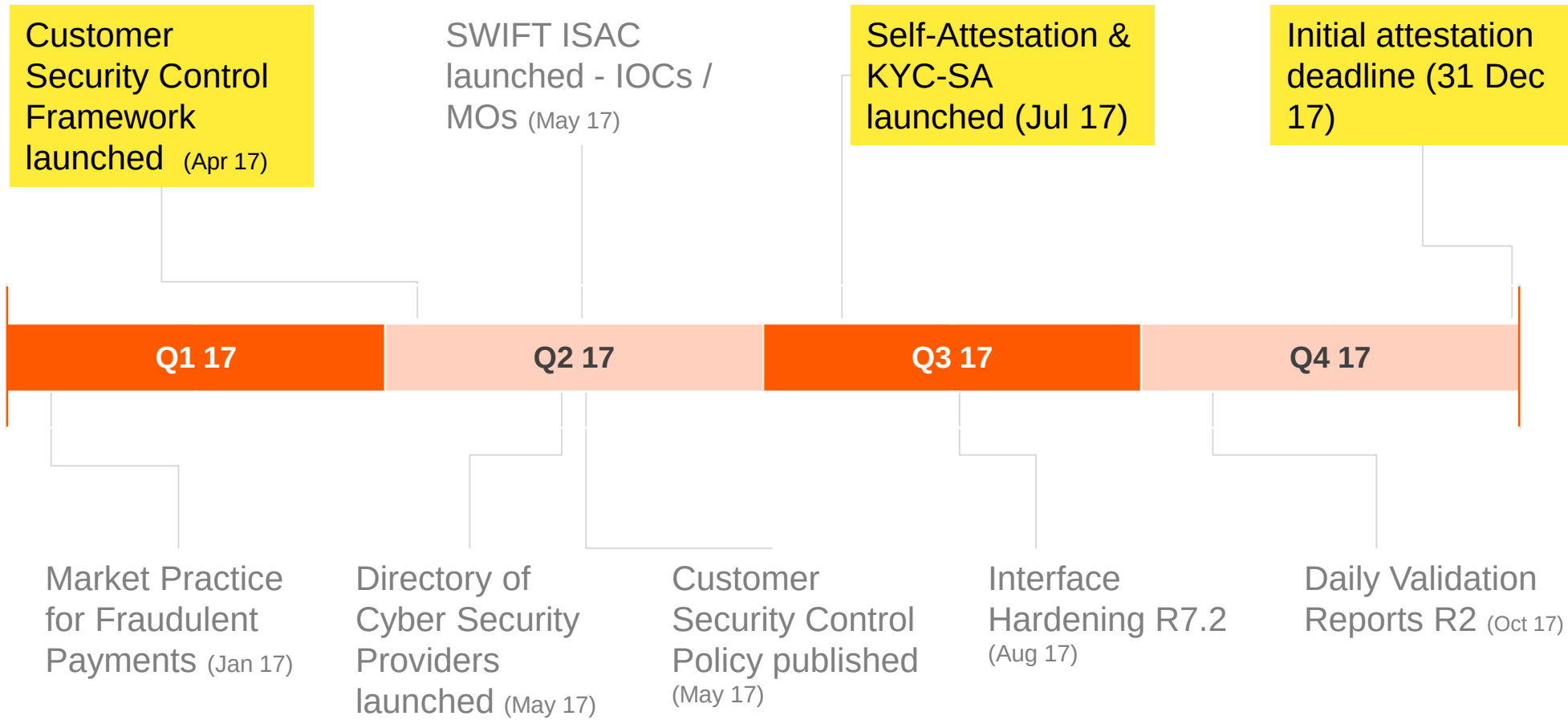
SWIFT Customer Security Program evolution

NEW TRENDS IN FINANCIAL TECHNOLOGIES: BLOCKCHAIN, CRYPTOCURRENCIES AND SECURITY

Pavel Prokudin, Account Director

Baku, 18th of May 2018

CSP update | 2017 milestones



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.

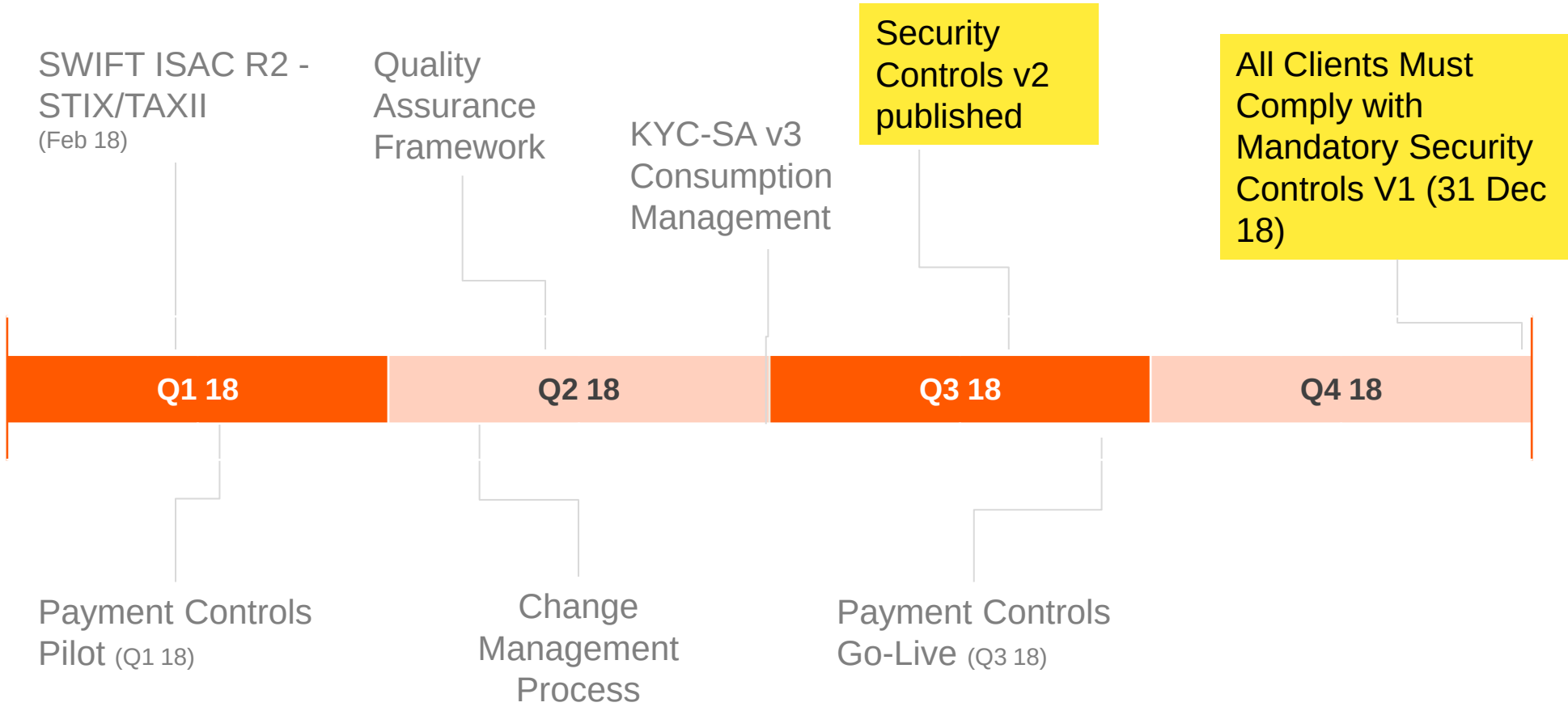
89%

BICs globally that self-attested by the deadline

99%

Attested BICs represent 99% of the FIN Traffic

CSP update | 2018 deliverables

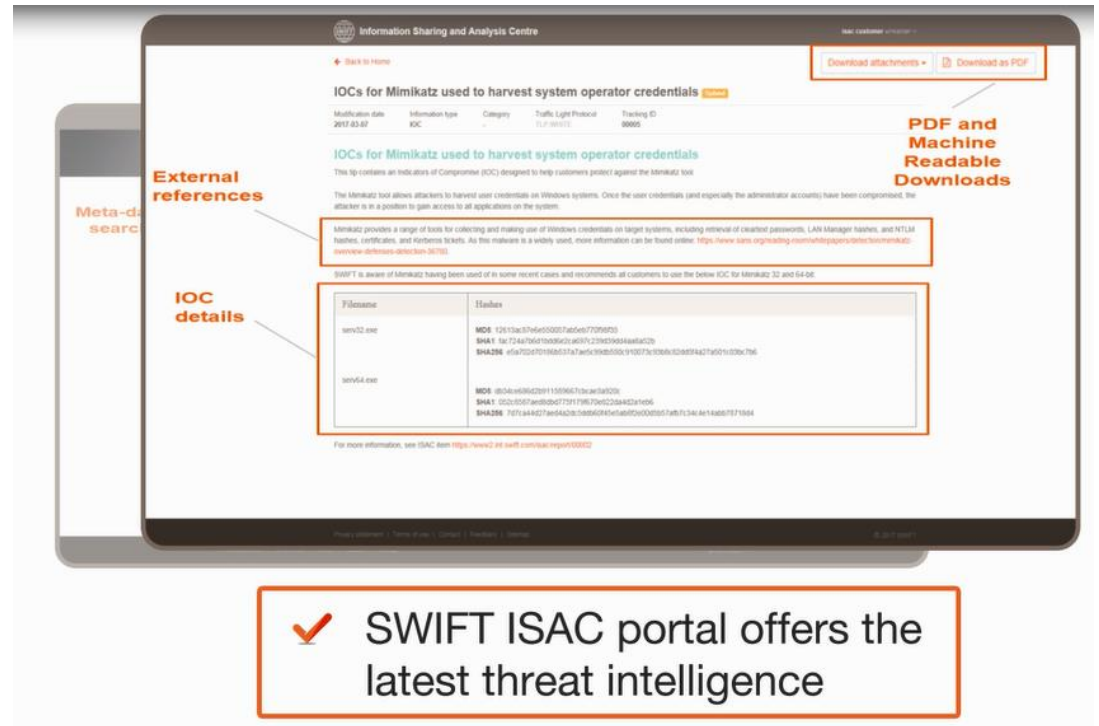


CSP update | SWIFT ISAC Portal

A 2nd release of SWIFT ISAC global information sharing portal was issued in February

This will enable the automated exchange of cyber-threat information using industry standard formats (STIX/TAXII) and allow access for non-SWIFT customers

The SWIFT ISAC continues to share threat intelligence with the community, including, indicators of compromise such as file hashes and details about malware samples observed. When possible, Modus Operandi used by attackers is described and machine-digestible files are provided (YARA rules, OpenIOC, etc.)



CSP | Quality Assurance

SWIFT has identified a set of risk indicators to track the overall effectiveness and quality of the Customer Security Controls Framework and associated activities (i.e., attestation, compliance, consultation)

If the risk indicators (either individually or collectively) suggests an underlying problem, SWIFT will evaluate the information, engage the community or segment, make a formal recommendation, and execute the appropriate corrective actions.

Each risk indicator has specific measurements to track the indicator. Additionally, the QA process will examine compound risk across multiple indicators.

- Risk thresholds will not be defined at this time.
- Additional insights will be captured through surveys and engagement with Users, Community groups, Vendors, Auditors & Consulting firms, and other stakeholders.

CSP update | Consumption

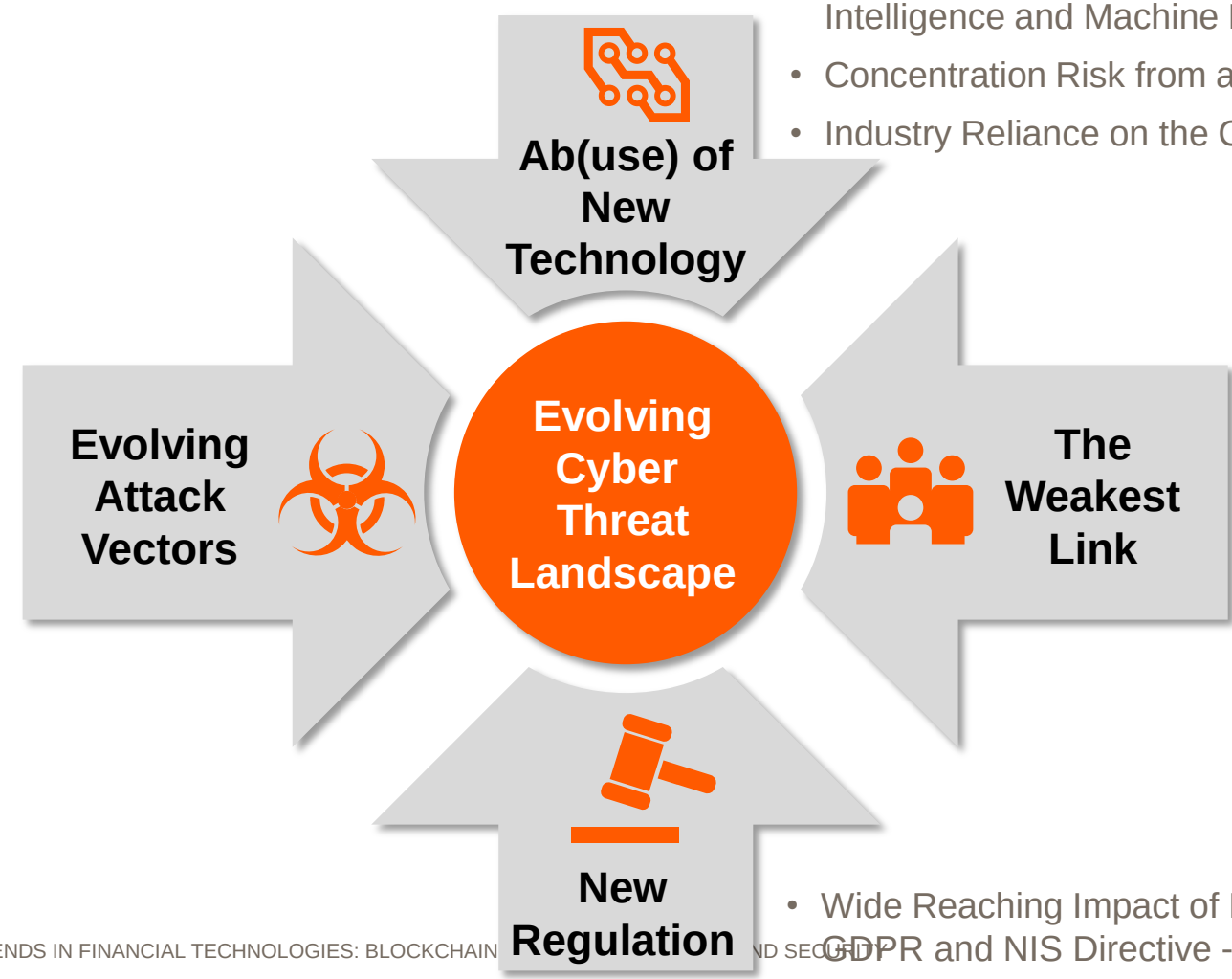
Users should consume counterparty attestation data and integrate this into their risk management and business decision-making processes.

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.

CSP update | Cyber attacks are intensifying

- Intense DDoS Attacks
- Rise in Ransomware
- Evolving Zero-Day (APTs) Advanced Persistent Threats
- Advanced Undetectable Malware
- Larger Data Breaches
- Targeting of Critical Infrastructure



- 'Arms-Race' as New Technologies Mature – Artificial Intelligence and Machine Learning
- Concentration Risk from a few Dominate Vendors
- Industry Reliance on the Cloud

- Endless (Spear) Phishing
- Rise in Insider Threats
- Race to Close the Gaps
- Deep Skills Shortage

- Wide Reaching Impact of New Regulation – e.g. GDPR and NIS Directive - Fines for PII Breaches

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.)

CSP & Transaction Pattern Detection

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

Daily Validation Reports – responding to the insider threat

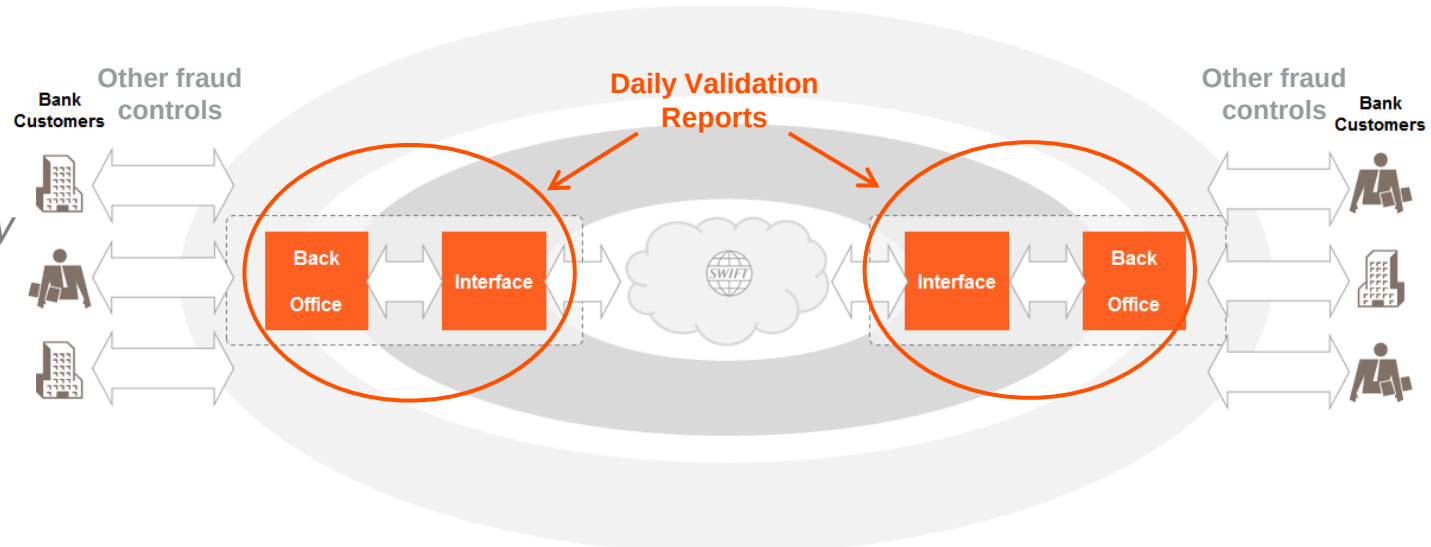
Step 1	Step 2	Step 3	Step 4
Attackers compromise customer's environment	*Attackers obtain valid operator credentials*	*Attackers submit fraudulent messages*	*Attackers hide the evidence*

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

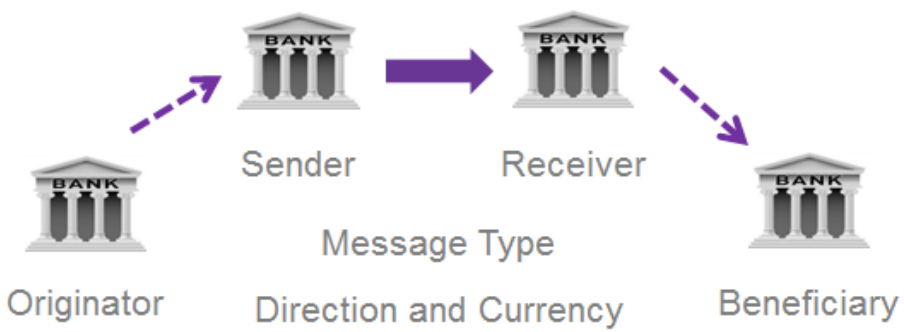
Daily Validation Reports - *provide a way to access SWIFT's record of transaction activity to mitigate this insider threat and not having to rely on, possibly compromised, interface systems.*

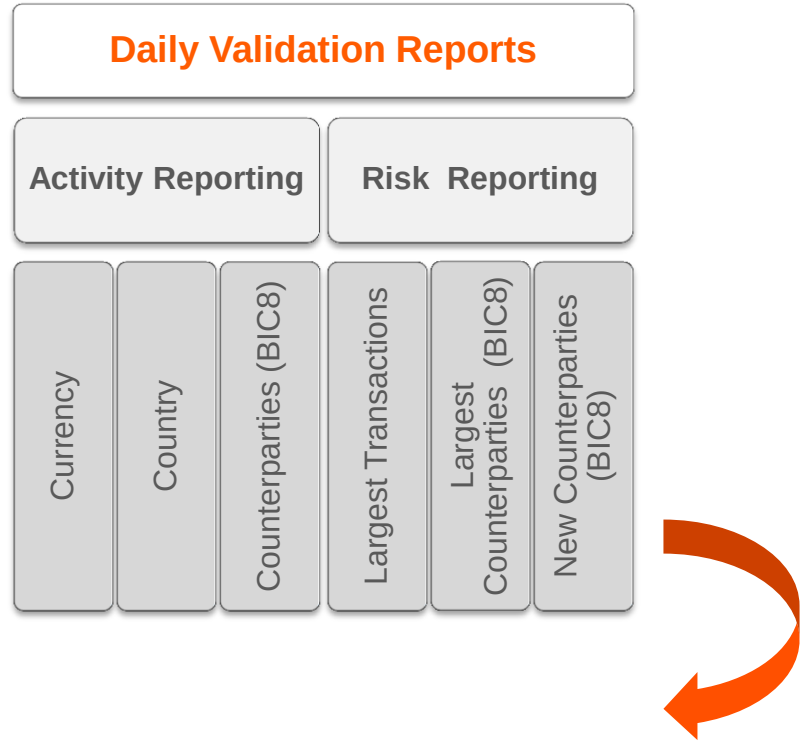


Daily Validation Reports

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

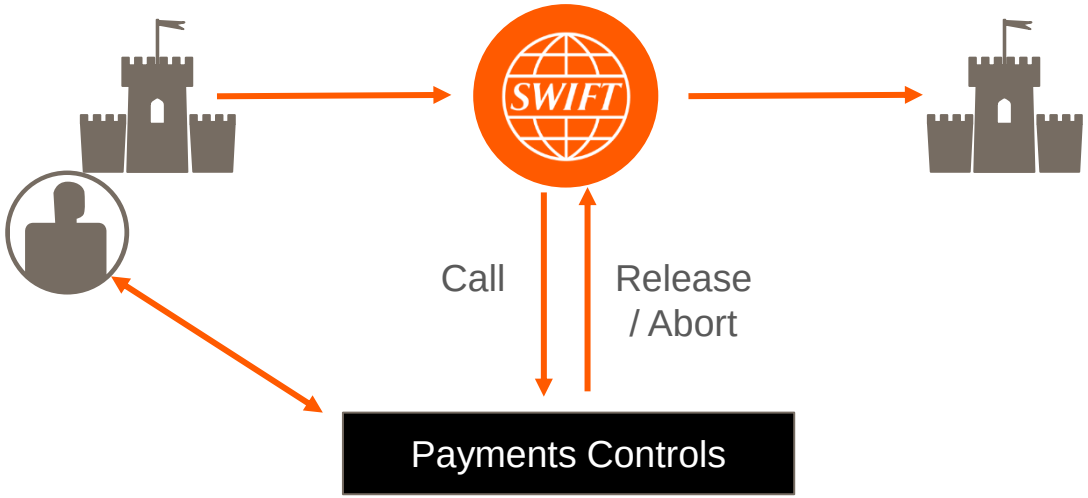




New Counterparties Reporting -
highlights any new combinations of direct and indirect counterparties. Makes it easy to identify new payment relationships that may be indicative of risk, and helps you quickly understand the values and volumes of the transactions involved

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)*

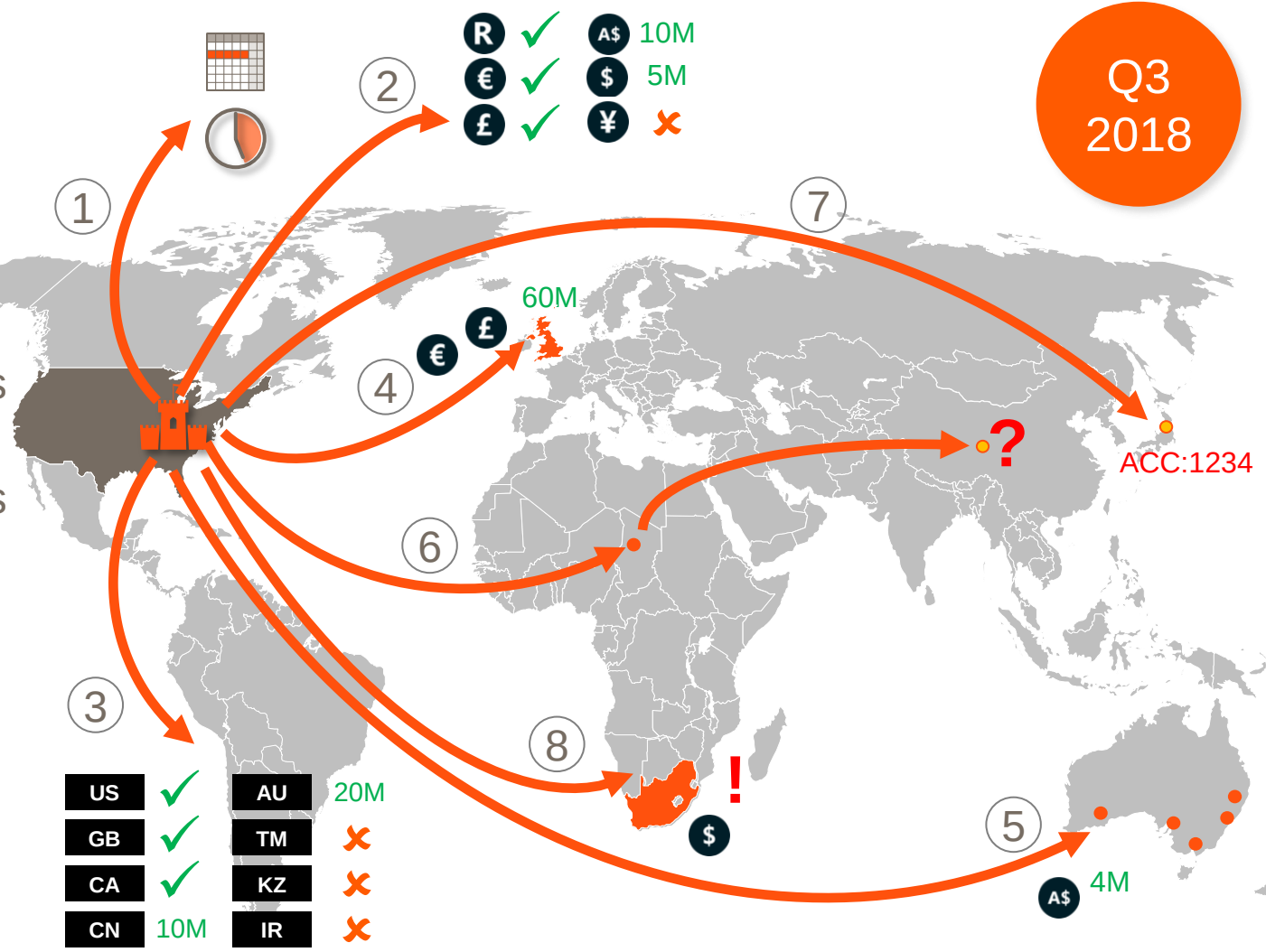
*Additional message types, including MX, are under consideration

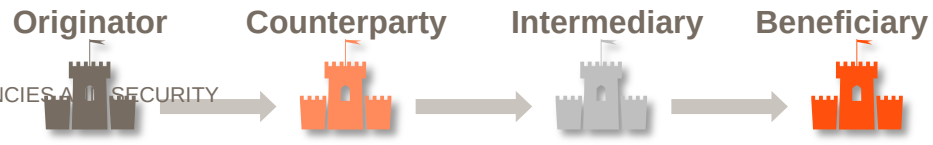
Payment Controls | **Capabilities**

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

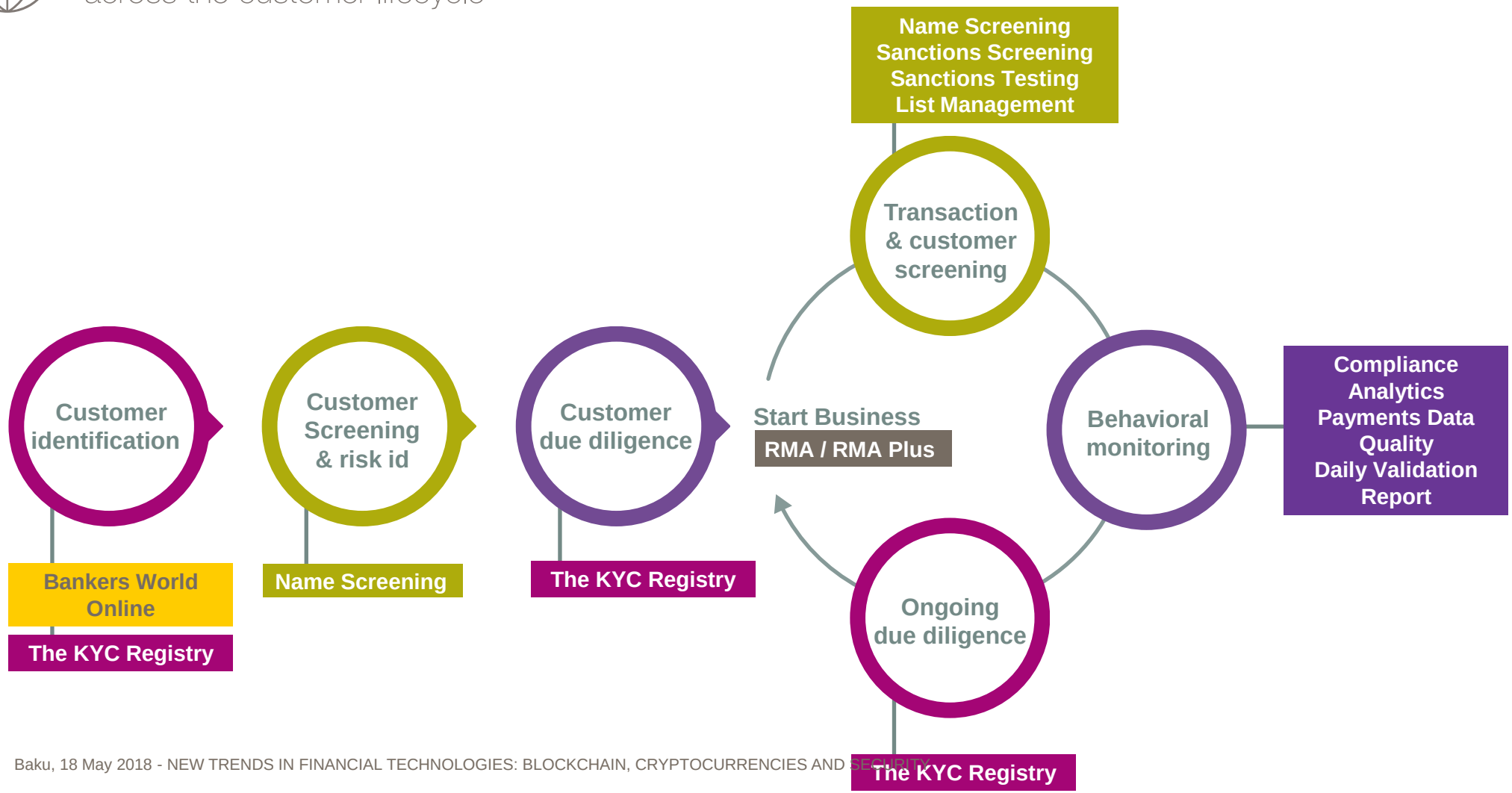
Across the complete payment chain





Financial crime compliance services

across the customer lifecycle



www.swift.com