SWIFT Financial Crime Compliance Initiatives

Compliance Services

Community-inspired financial crime compliance solutions

Key compliance challenges

The payment landscape is changing with major market infrastructure overhauls, more sophisticated customer demands and new technology. Compliance teams are under increasing pressure to ensure their businesses remain competitive whilst staying compliant.

No. 1 threat to business growth

CEOs see over-regulation as the top-ten threat to business growth.*

Compliance in a real-time world

Convergence of compliance & fraud prevention

Data-driven analytics

*PWC 22nd annual CEO survey 2019

Addressing a clear community need

- Relevant to all SWIFT users (all geographies)
- Significant costs at stake
- Not a competitive area

Started small – scaling fast

- Initial community discussions in 2009
- First services launched in 2012
- Now 11 services live – More than 5500 institutions

Strategic for SWIFT and community

- A key pillar of our SWIFT2020 strategy
- Around 200 SWIFT employees dedicated
- Significant financial investment
- Long-term approach

With a targeted scope

- Sanctions
- KYC
- AML
- Fraud detection

Leveraging SWIFT truly distinctive assets

1. Community/Reach (10,000 FIs & Corporates)
2. Standards and market practices
3. User-controlled access to transaction flows
4. Not-for-profit, scale economies business model
5. Community-driven innovation model (co-creation)

Community-inspired integrated financial crime compliance utility

Single inter-connected utility for the complete FCC lifecycle

- Offering a ***comprehensive range of compliance products*** for KYC, Sanctions, Fraud Prevention, and AML for on-boarding and on-going risk management and due-diligence
- Addressing, over-time, the ***needs of the whole SWIFT community***
- ***Interconnected through APIs*** to leverage features, analytics and data between products, and ensure best user experience
- Open, through APIs, to ***integrate with other customer and vendor solutions***
- ***In the SWIFT secure cloud*** to mutualise cost, improve standardisation, reduce deployment time and provide transparency

Financial Crime Compliance | Key achievements

The KYC Registry has **5,500** financial institutions registered and contributing data across **200 countries** and territories worldwide.

SWIFT has **invested in and extended** its range of compliance offerings consistently since 2012.

We added three new products in 2017: **Correspondent Monitoring, Daily Validation Reports** and **Name Screening** batch.

70+ institutions are ensuring effectiveness and efficiency of their sanctions filters with SWIFT **Sanctions Testing**

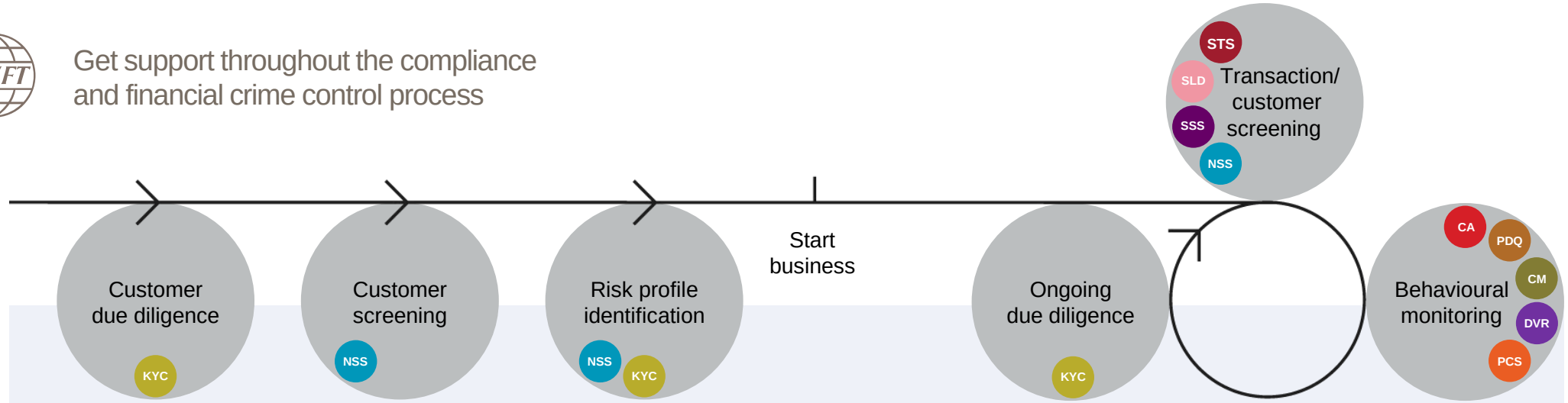
Sanctions Screening has **950+** institutions screening messages in-network and through direct back-office connectivity. **Making SWIFT one of the largest transaction screening providers.**

Compliance Analytics is changing the way that over **70** institutions analyze and mitigate their correspondent banking risk.

We introduced Fraud prevention systems in real-time : We are helping over **300+** institutions to protect themselves against fraud with **Payment Controls** and **Daily Validation Reports**

Financial Crime Compliance | Complete lifecycle

Get support throughout the compliance and financial crime control process



KYC **The KYC Registry** provides a secure, shared platform for financial institutions to exchange standardised know your customer information.

NSS **Name Screening** gives you a hosted, flexible filter suite, expert list management and ongoing quality assurance, all with the simplicity of using a search engine.

SSS **Sanctions Screening** provides fully-managed, securely-hosted screening of your message traffic against the latest sanctions lists, with instant alerts of any matches.

SLD **Sanctions List Distribution** supports sanctions compliance, with up-to-date lists, ready for download in standardised XML format.

STS **Sanctions Testing** provides automated, independent testing for better, smarter transaction, customer and PEP screening.

CA **Compliance Analytics** pinpoints compliance risks across your operations and correspondents with our global, group-level payments analysis.

PDQ **Payments Data Quality** supports compliance with FATF Recommendation 16 guidelines for originator and beneficiary information.

CM **Correspondent Monitoring** gives a new way to monitor your correspondents activities to identify activities indicative of money laundering

DVR **Daily Validation Reports** help supplement your existing fraud controls by providing an independent daily snapshot of your SWIFT transaction activity.

PCS **Payment Controls** helps you manage your payment policy and identify unusual or uncharacteristic payment risks.

SWIFT Community & KYC registry

Compliance Services

Community-inspired financial crime compliance solutions

Driven in partnership with leading Financial Institutions

Promote Standards

the Wolfsberg Group

Drive Adoption

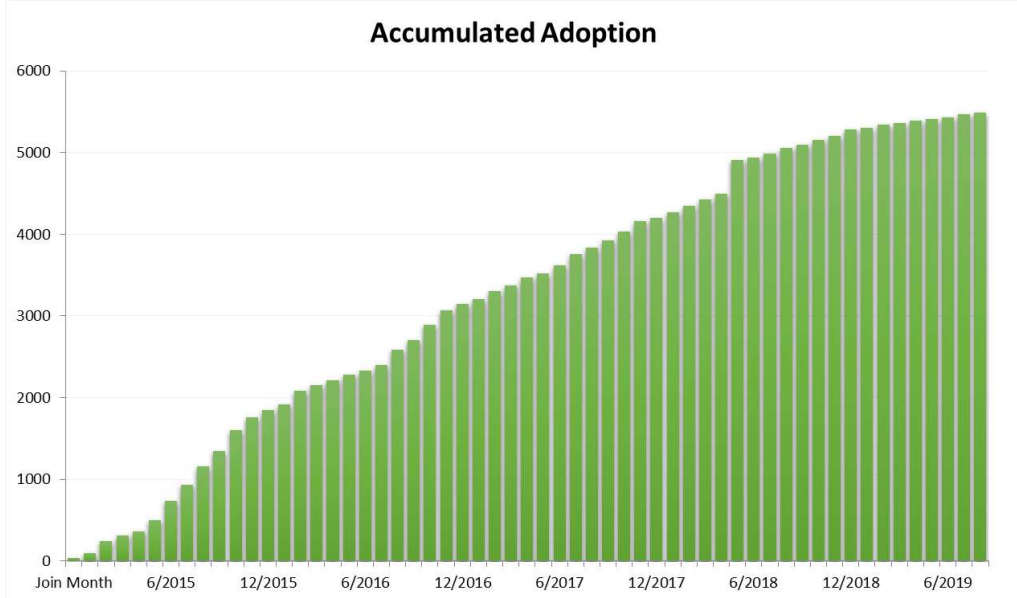
Design Roadmap

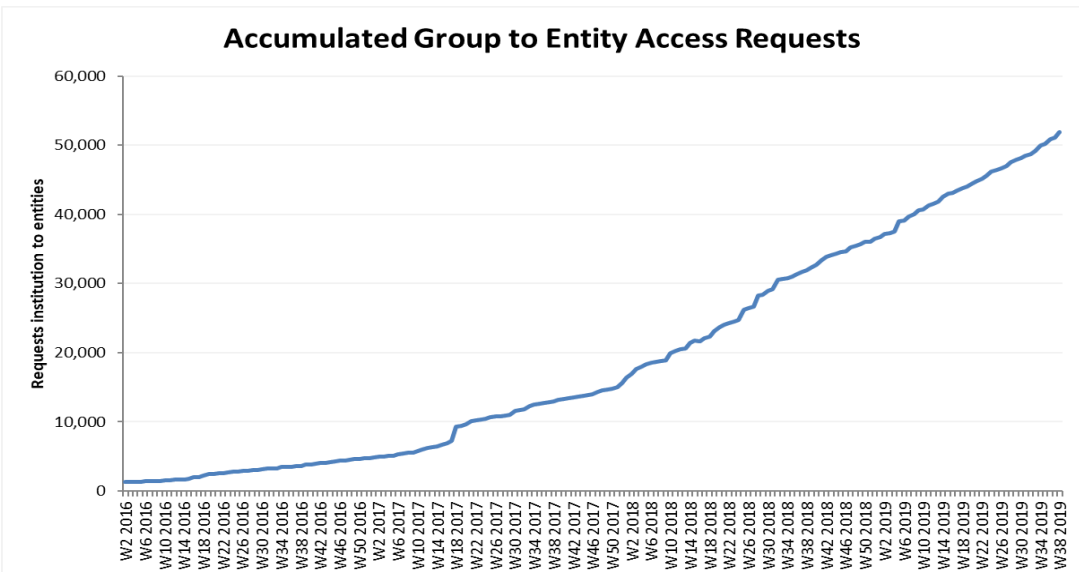
Validate Features

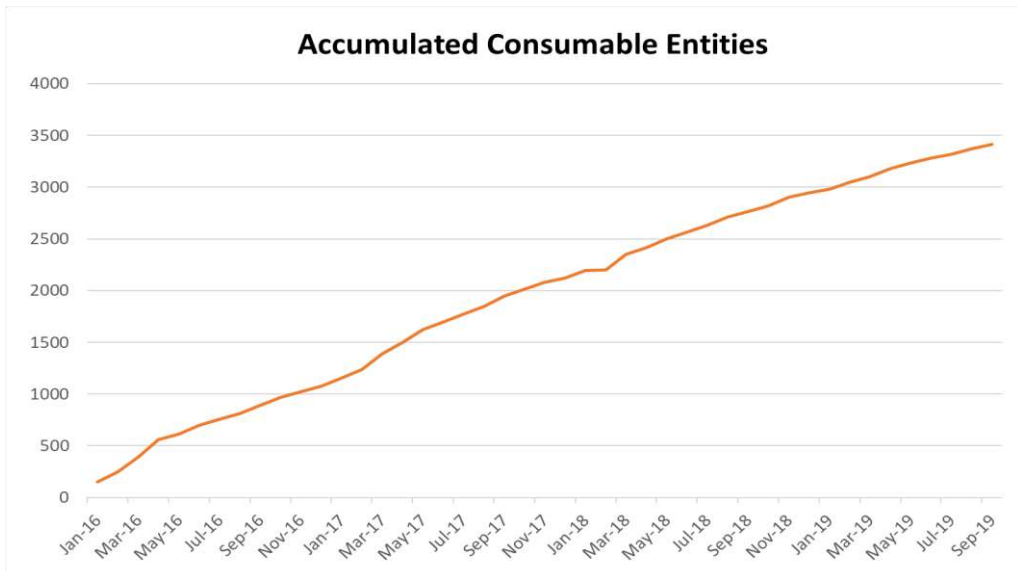
KYC Registry Today

More than 5,500 financial institutions representing more than 2,100 banking groups

- **2,400 +** in Europe, Middle East and Africa
- **1500 +** in Asia Pacific
- **1500 +** in the Americas & UK
- **200 +** countries and territories worldwide
- **77** Central Banks & Monetary Authorities







The KYC Registry – The five Pillars of Trust

Confidential, user-control access:

2-Level access granting for:
Basic: CDD KYC data and documents including 2017 Wolfsberg Due Diligence Questionnaire
Extended: Additional information related to enhanced due diligence EDD

Standardized KYC Baseline

Efficient: All KYC data provided by counterparties available as **electronic data** and in **same format and structure**

Up-to-date information

Current: Time-stamped data and diligent update requirements. **Any changes to client data are communicated to all counterparties in real-time**

Data verification by SWIFT

Correct and accurate: All data is time-stamped and verified and validated by SWIFT compliance professionals

Cooperative business model

Fair: Free upload of own KYC data, free validation and publication by SWIFT, unlimited number of users
Transparent volume based pricing for consumption and capped maximum spend

How your correspondents use KYC registry?

***Spending 72% less time on due diligence checks & exchanges**

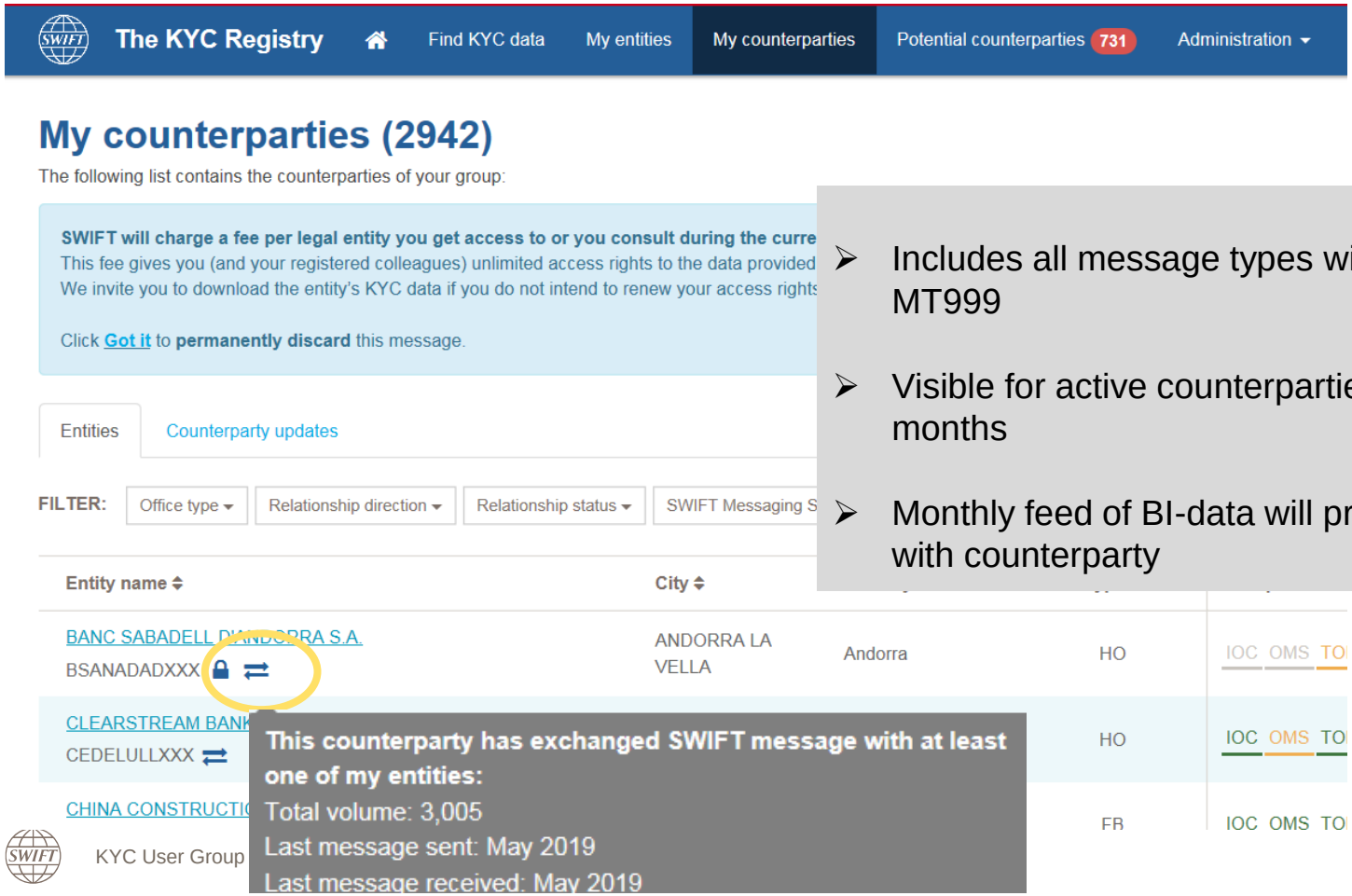
***HSBC report on KYC registry**

- Bulk Access request and granting
- RMA indicator
- Potential counterparties
- APIs
- KYC Registry Messenger
- Messaging export
- Wolfsberg CBDDQ alignment
- One standard baseline for all clients
- KYC Registry profile in xls
- Corporates

Increasing the visibility & Expending business relationships

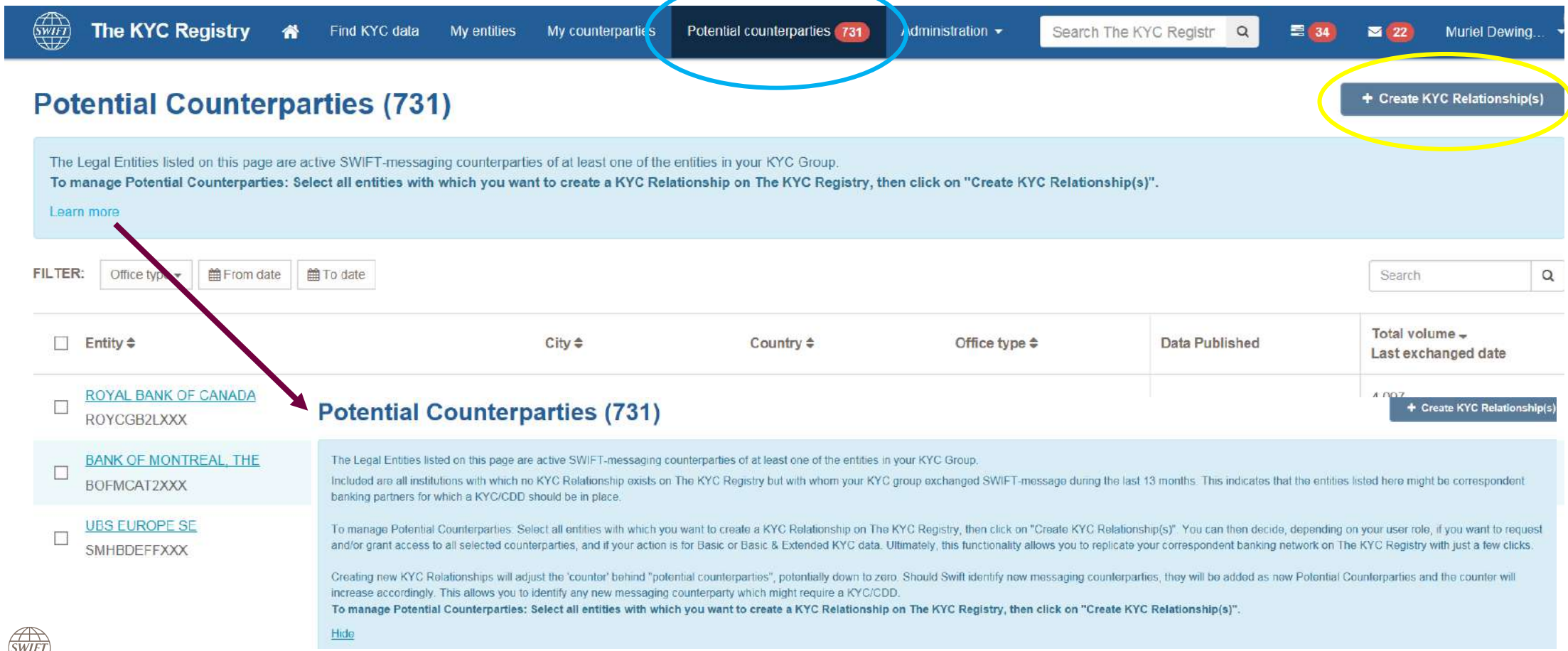
Fast & Safe Exchanges!

Display of Messaging Counterparty

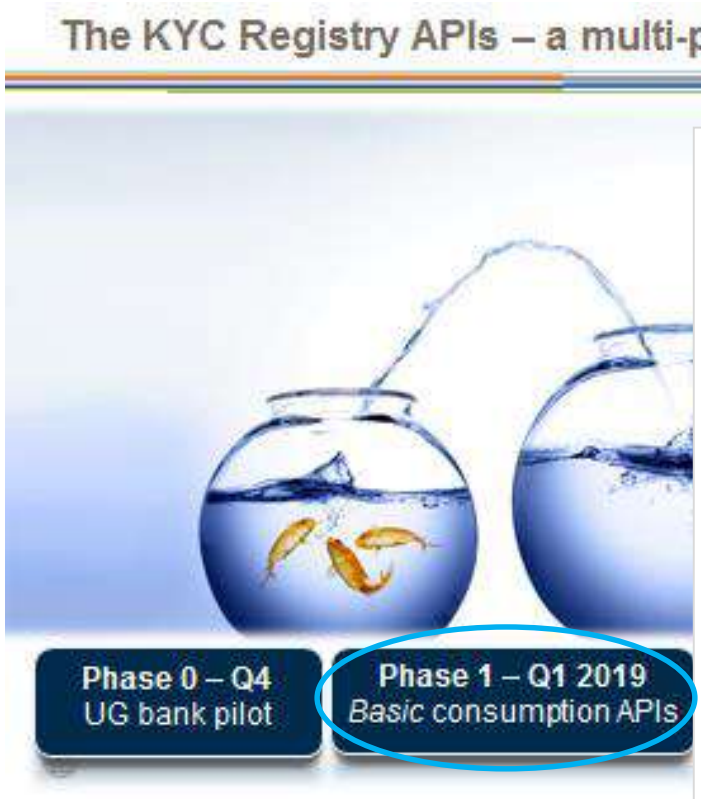


- Includes all message types with exception of MT0xx and MT999
- Visible for active counterparties with traffic during last 13 months
- Monthly feed of BI-data will provide indication about activity with counterparty

Potential counterparties



API




```
{
  "category-data": {
    "entity-data": {
      "Identification Of Customer: data":
        "LocalLegalName": "Global Bank",
        "ImmediatePreviousLegalName": "Pre
        "LastLegalNameChangeYear": 1990,
        "LocalTradingName": "This is a Tes
        "AdditionalTradingName": "This is
        "LocalLegalForm":
          {"Cooperative"},
        "AnglicisedLegalForm":
          {"Cooperative"},
        "IndustryClassification":
          {"SIC"},
          {"NAICS"},
        "SicCode":
          {"6021 - National Commercial Banks"},
          {"6035 - Savings Institutions, Federally Chartered"},
        "NaicsCode":
          {"522130 - Credit Unions"},
          {"522220 - Sales Financing"},
        "EmployeesNumber":
          {"201-500"},
        "RegistrationNumber": 1234532,
        "RegistrationAuthorityCountry":
          {"Germany"},
        "RegistrationAuthority":
          {"Unternehmens-register - Company Register"},
        "IncorporationDate": "1975-04-25",
```


- Streamlined data fields & documents IDs
- Availability of the full KYC Profile (including unanswered questions)
- Publication date & baseline version available for each category
- All document parameters displayed (e.g. expiry date, language, description)
- Only granted data can be extracted
- Only the latest published version of the baseline folders can be extracted

Add-on: DJ FACTIVA Adverse Media Module

Competitive license fee

Flat yearly fee

Unlimited number of users

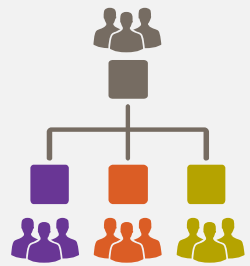
All KYC Registry users of a bank subscribing to KYC Adverse Media receive access

Unlimited number of articles

There is no limit on the volume of articles consumed per year

License covers all entities in KYC Group

All entities under the same KYC Registry contract have access to KYC Adverse Media



Do you know?

Flexible invoicing model:

1- FREE: Registration+ Membership+ publication + validation+ support

2- Pay as you go model if you request access to another institution's documents.

3- CAPPED invoice for unlimited usage; no matter how much used, the cap can't be passed

4- Fixed FEE model- I want to pay less and do bulk accesses.

UNLIMITED USERS ➔ FREE ***(why not to add other departments?)***

Training your users 24/7 on KYC ➔ FREE (SWIFTSmart)

Inviting other banks to KYC registry?

Exchanging Emails & messages over KYC – YES!!

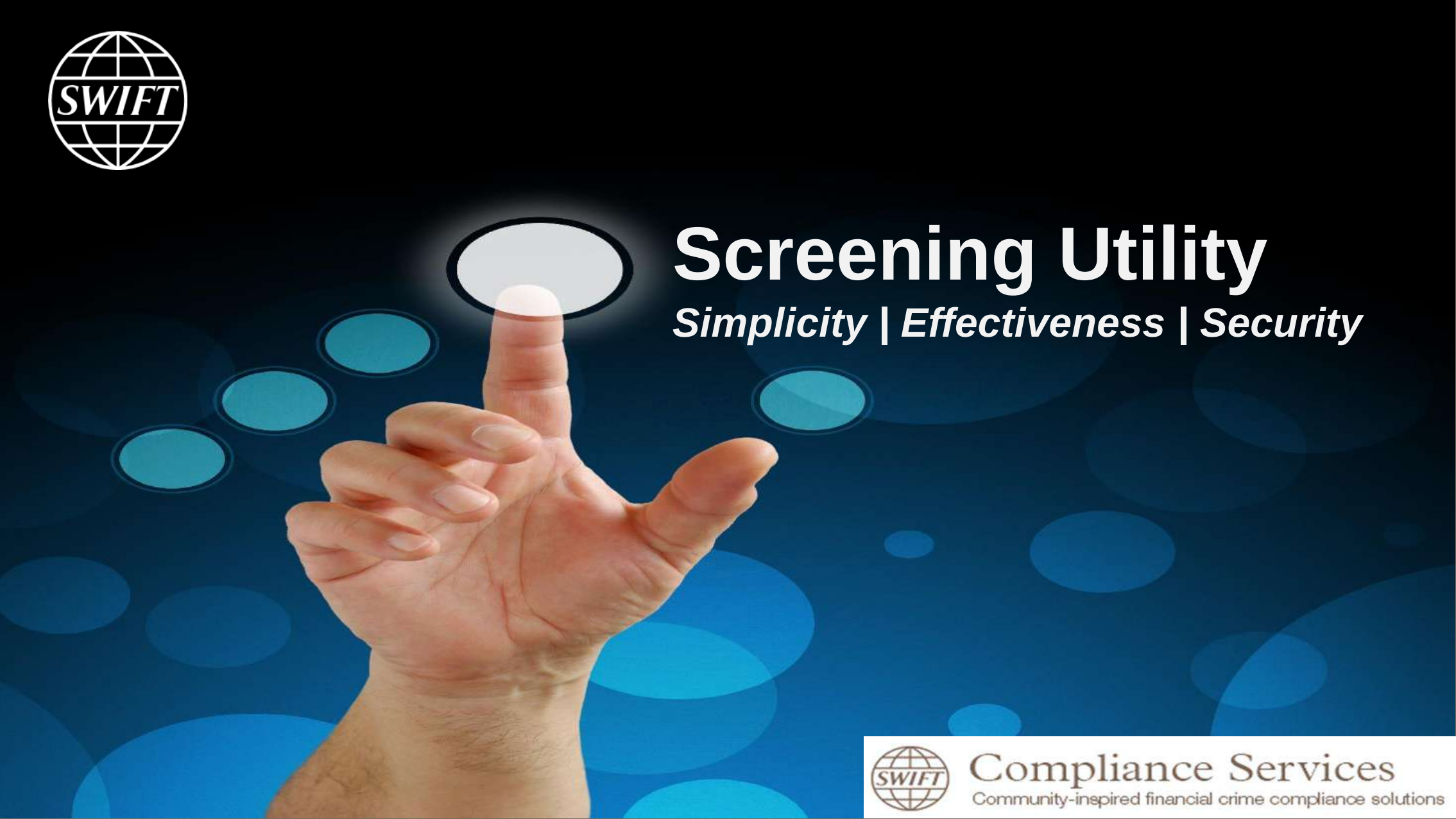
The KYC Registry on SWIFTSmart

SWIFT has developed online training material enabling you to learn about The KYC Registry and understand the different facets of the product. The courses, accessible through our SWIFTSmart platform, are available to all swift.com accounts holders for free (access via single sign-on and accessible from any secure internet connection, unlimited number of views).

Introductory	Who should attend?	Where to find it?
The KYC Registry Video	All swift.com users	Click here

The KYC Registry curriculum	Who should attend?	Where to find it?
Module 1: Introduction to The KYC Registry	All KYC users	Click here
Module 2: The KYC Registry Baseline	All KYC users	Click here
Module 3: The KYC Registry Administration	KYC Administrators	Click here
Module 4: The Contribution Process	KYC Submitters & KYC Approvers	Click here
Module 5: The Qualification and Publication Process	All KYC users	Click here
Module 6: The Consumption Process	KYC Requesters, KYC Viewers & KYC Granters	Click here

About SWIFTSmart: SWIFTSmart is an interactive, cloud-based service that provides a full catalogue of courses. It offers more than 200 courses in multiple languages, helping you to obtain knowledge about most of the SWIFT products and services and enabling you to learn more about industry topics.


Screening Utility
Simplicity | Effectiveness | Security
Compliance Services
Community-inspired financial crime compliance solutions

Ready-to-Run solutions protecting your business

Name Screening

Supports your KYC process

Internal Databases

IDENTIFY THE RISK

Identify the risk each supplier exposes you to and mitigate it based on your risk policy.

- Sanctions & SOR
- PEP & RCA
- Adverse Media
- Private list

Transaction Screening

Spots & intercepts potential sanction breaches

Incoming & Outgoing Transactions

PROTECT YOURSELF & YOUR COUNTERPARTIES

Protect yourself from the risk each transaction exposes you to.

- Sanctions & SOR
- Private list

Fraud detection

Adds-on a layer of Security to prevent Frauds

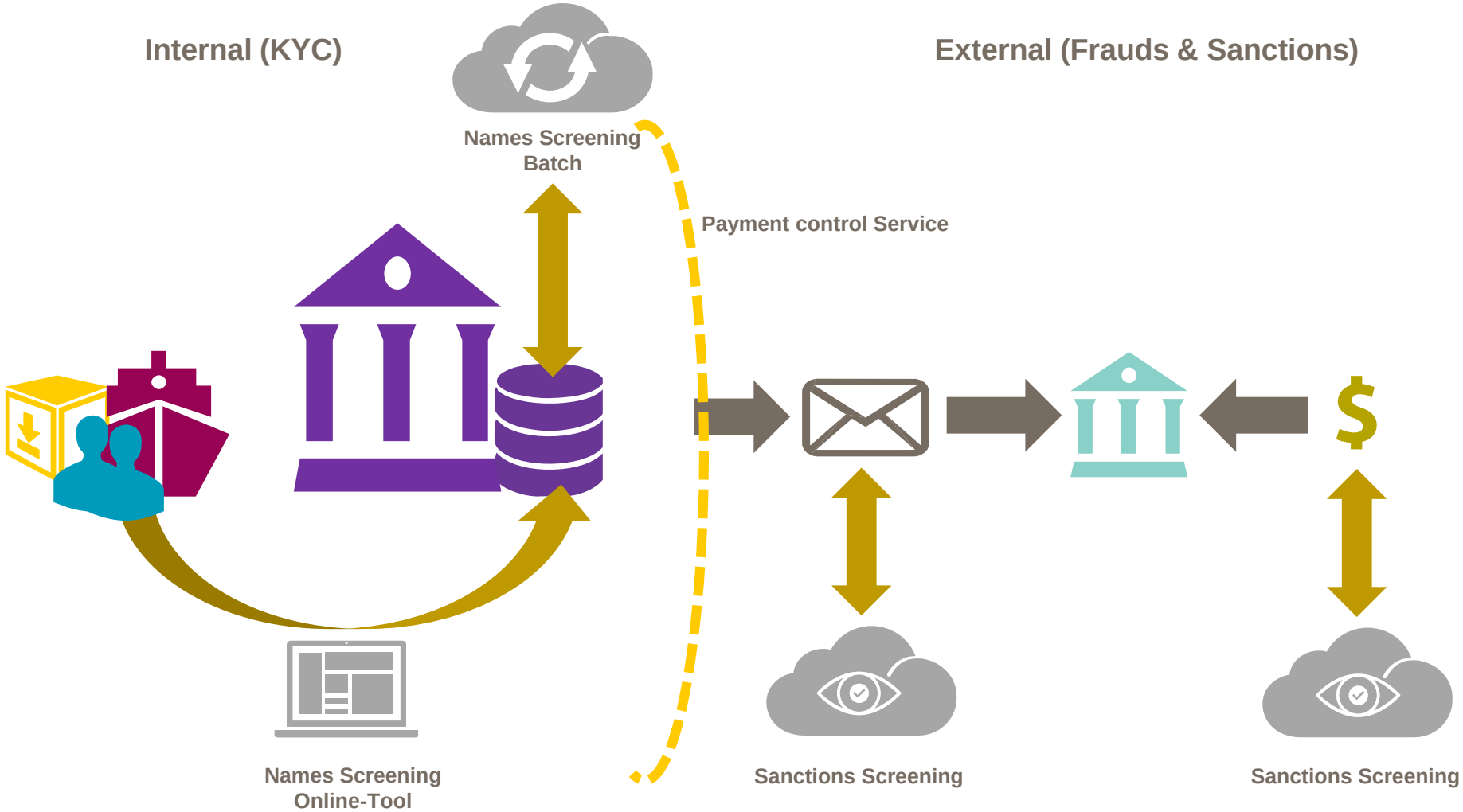
Outgoing Transactions

Detect animalises and potential FRAUDS

Gain understanding about your own activities and detect abnormal behaviours

- Currencies & amount
- Corridors, Institutions & account
- Timing
- Individuals & aggregated

Ready-to-Run solutions protecting your business



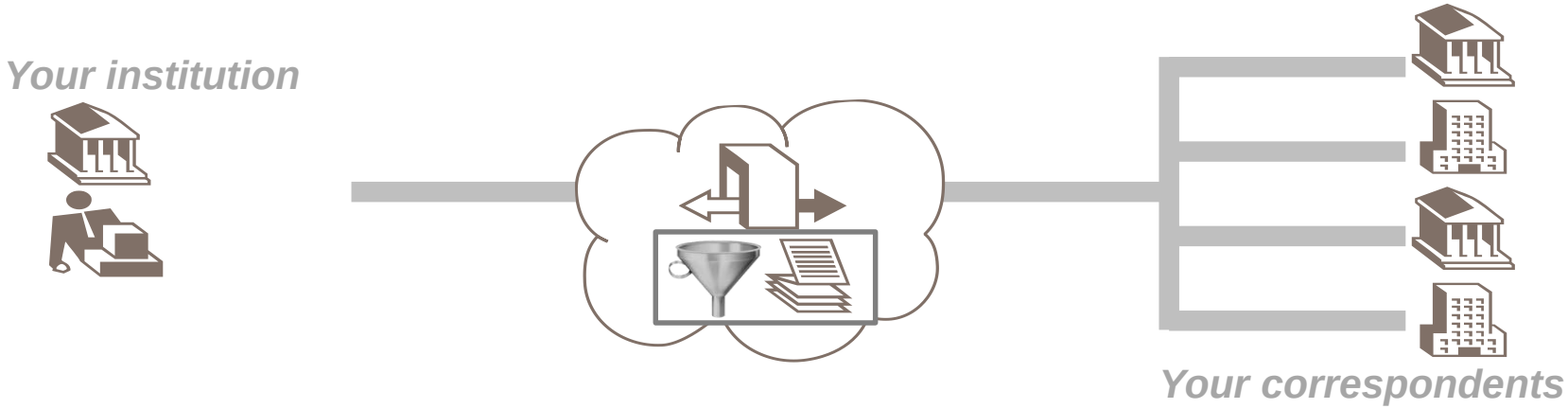
Sanctions Screening Services

Compliance Services

Community-inspired financial crime compliance solutions


FStech
awards 2015
Sanctions Screening wins FStech award for Compliance
SWIFT honoured for "Compliance Project of the Year"
40+
central
banks
950+
Clients
200+
countries

Sanctions screening over SWIFT



- Screening engine & user interface
- Centrally hosted and operated by SWIFT
- No local software installation & integration
- Real-time
- Sanctions List update service

Public Sanctions lists available

50+

Public sanctions lists updated by SWIFT daily

Private lists & Good-guys lists managed by the users

AND

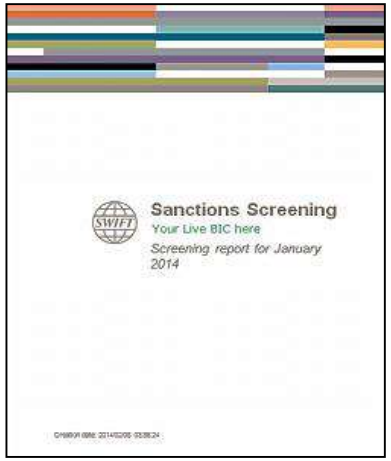
Research-based ownership lists

Country	Description
Australia	Department of Foreign Affairs and Trade (DFAT)
	DFAT Autonomous list
	DFAT Country Embargoes
Canada	Office of the Superintendent of F.I. (OFSI)
	OSFI - United Nations Act Sanctions
	Department of Foreign Affairs and Trade (DFAIT)
	DFAIT Countries Embargoes
European Union	European Official Journal
	EU Countries Embargoes
	EU Ukraine Restrictive Measures
France	Journal Officiel français
Hong Kong	Hong Kong Monetary Authority (HKMA)
	HKMA Countries Embargoes
Japan	Ministry of Finance
	Special Measures
Netherlands	Frozen Assets List - Dutch Government
New Zealand	New Zealand Police
China	Ministry of Public Security of the PRC
Ukraine	State Financial Monitoring Service of Ukraine
	National Security and Defense Council

Country	Description
Norway	Ministry of Foreign Affairs (MFA) list
	MFA United Nations list
	MFA Countries Embargoes
Singapore	Monetary Authority of Singapore - Investor Alert List
	Terrorism (Suppression of Financing) Act
Switzerland	Secrétariat d'Etat à l'Economie
	SECO Countries Embargoes
United Kingdom	Her Majesty's Treasury
	HMT Countries Embargoes
	HMT Ukraine Restrictive Measures
United Nations	United Nations
	UN Countries Embargoes
United States of America	Financial Crimes Enforcement Network (FINCEN)
	OFAC Specially Designated Nationals
	OFAC Embargoed Countries
	OFAC non-Specially Designated Nationals, including: • OFAC Palestinian Legislative Council • OFAC Part 561 • OFAC Foreign Sanctions Evaders • OFAC Sectoral Sanctions Identifications • OFAC Non-SDN Iranian Sanctions Act

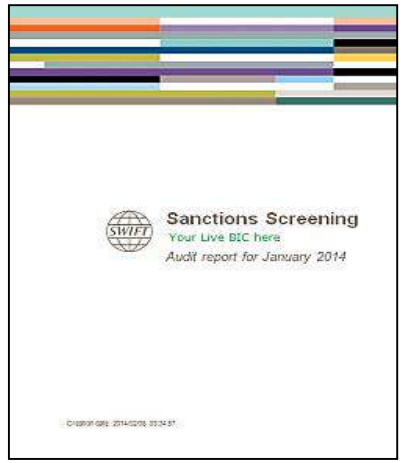
Report tools:

Screening Report



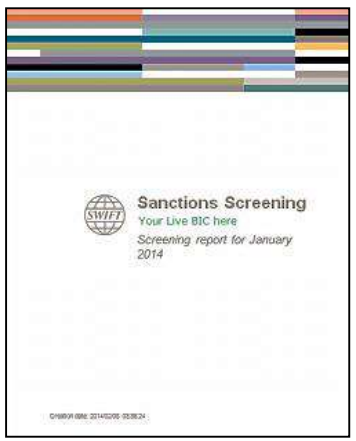
- Copy of each alerted transaction
- Hit details
- Final status
- Monthly (to be saved and stored)
- rtf & XML format

Audit Report:



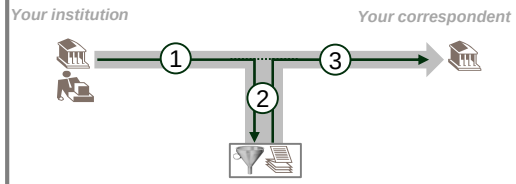
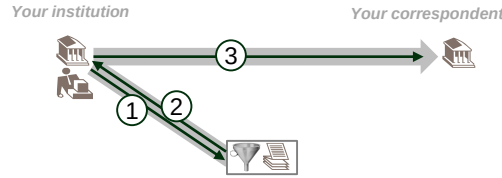
- Audit log of all transactions screened
- Audit log of all operators activity and decisions
- Comments
- Monthly and weekly (since July 2016)
- Rtf format

Quality assurance Report



- Annual quality assurance checks on effectiveness of the service
- Verifies that lists used mirror regulatory sources
- Measures exact and fuzzy matching capabilities
- Provides details on filter configuration and related impact
- Upon request

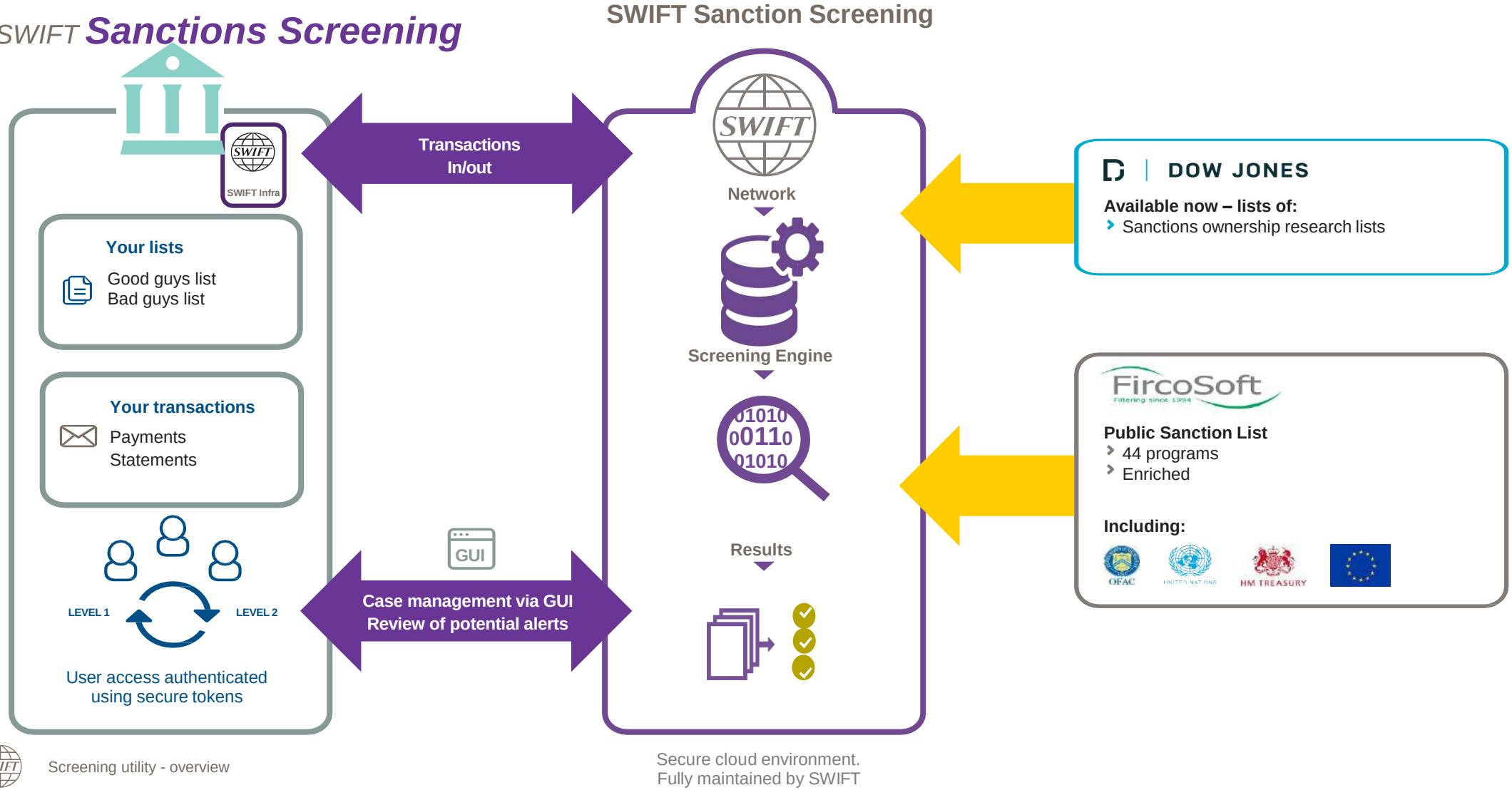
Sanctions Screening : Implementation options

		Copy option	Connectors option
			
		Transparent routing of FIN transactions to the service using FIN-Copy	*Query/response of all transaction types through API call to the service* *Screen or Screen and Send mode*
			Connector on SAA
Timeframe	*Time to compliance*	**Few weeks for prod** **One month min**	**Few Months**
Footprint	*Installation & integration*	**Zero***	**Limited (IPLA in SAA)**
Flexibility	*Granularity on what is filtered*	**Limited**	**Unlimited (routing inherited from SAA)**
Scope	*Transactions Screened*	**All cat beside cat8**	**All SWIFT transaction types*** **SEPA messages and any formats****

*Except MT 0xx

How does it work

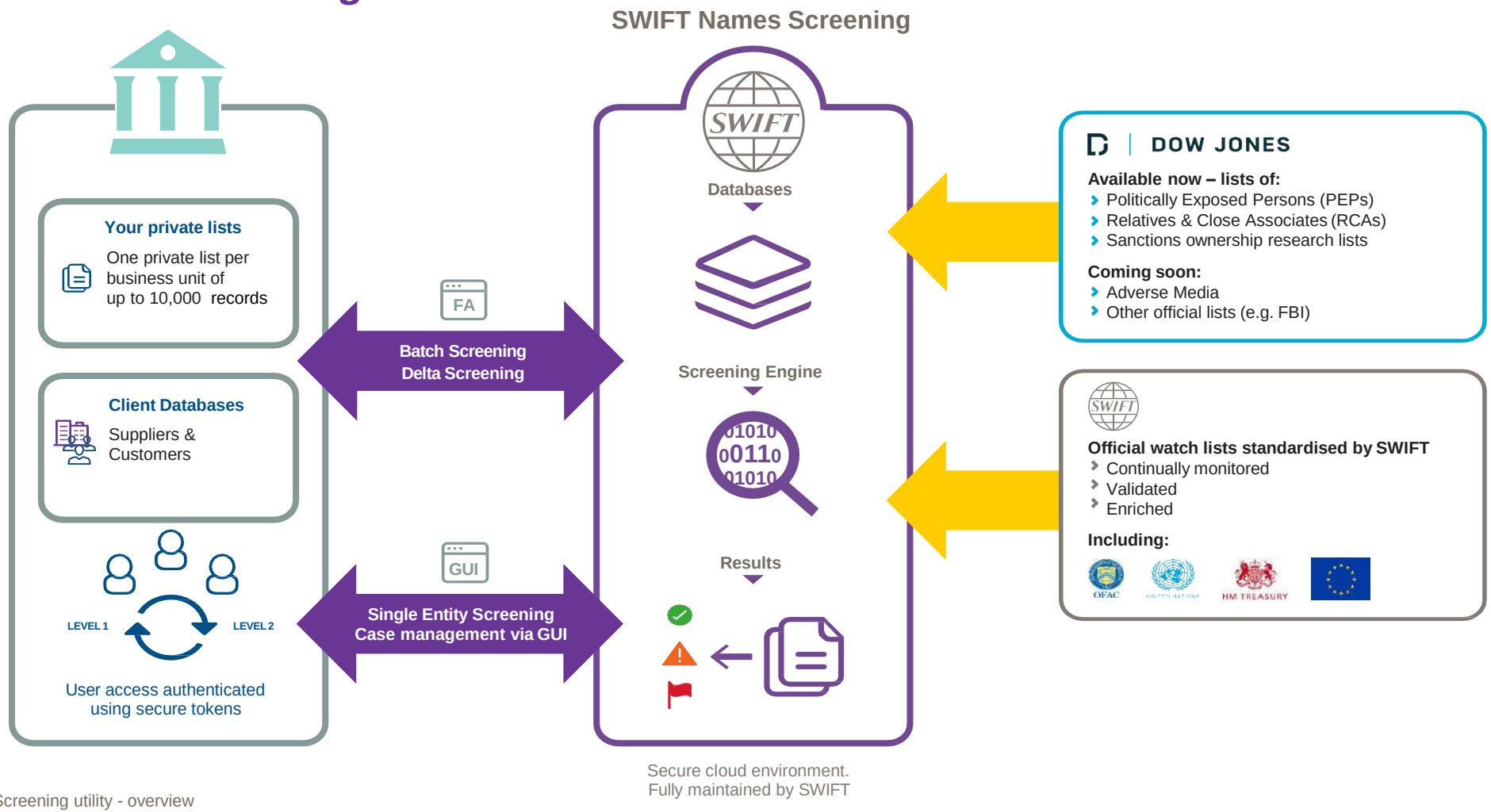
SWIFT Sanctions Screening




SWIFT
Name Screening against PEPs
& Sanctions

How does it work

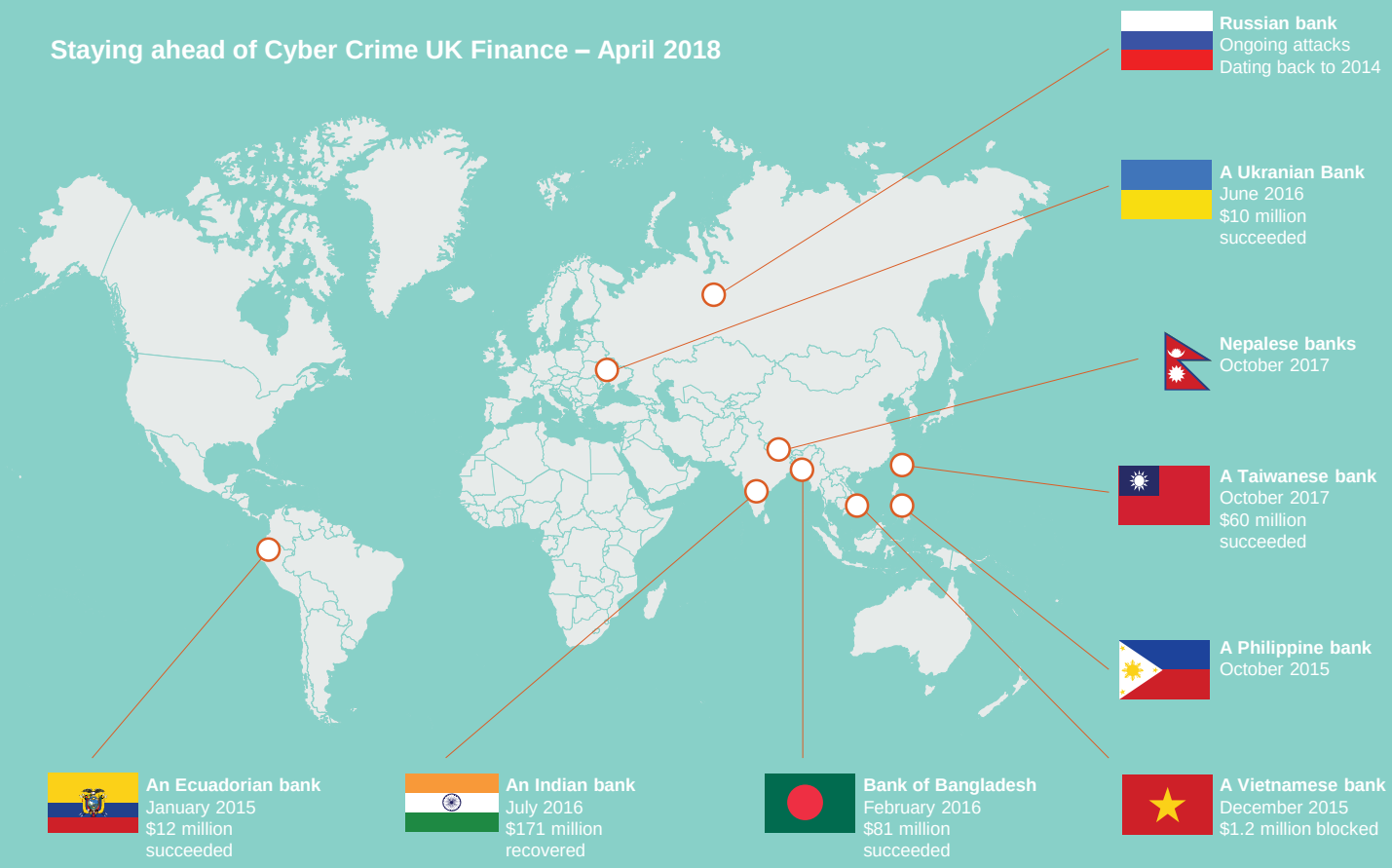
SWIFT ***Name Screening***




Fraud Prevention:
Payment controls Services
Compliance Services
Community-inspired financial crime compliance solutions

Financial institutions and payment infrastructures are the new targets

Source: 2017 Payment threats and fraud report, European Payments Council



Cyber-security Regulation[1] for the Financial Industry

USA
- Executive Order - Strengthening The Cybersecurity of Federal Networks And Critical Infrastructure
- FDIC, OCC and FRB Agencies - Enhanced Cyber Risk Management for FIs
- New York State Department of Financial Services - Cybersecurity Regulation

G7
- Principles and Actions on Cyber
- Fundamental Elements of Cybersecurity for FIs

CPMI
- Guidance on Cyber Resilience for FMIs – 2 Hour Recovery

SWIFT G10 Oversight Forum
- Reinforcing Cyber Resilience of FIs
- Mandatory Controls

EU- European Union NIS directive "Cyber security strategy applicable to all member states"

Non EU but Europe continental countries updating the payment regulations with cyber security fraud prevention rules

Brazil
- New national digital security strategy

South Africa
- Cybercrime and Cybersecurity Bill

Pan-Europe
- EC - Directive on Security of Network and Information Systems (NIS Directive)
- EC - EU Strategy for Cybersecurity
- ECB - Reporting Framework for Cyber Incidents
- ECB - Cyber Resilience of the EU Ecosystem
- EBA Guidelines on Risk Assessment under SREP
- European Securities Market Authority (ESMA)

Russian Federation
- Temporary Regulation on information exchange
- Financial sector cyber incident reporting
- Central Bank of the Russian Federation (CBRF) - Cybersecurity State Standard (GOST)
- Information Security Doctrine
- Security of Russia's critical information infrastructure

China
- Cyber Security Law of the People's Republic of China (CSL) regulation of network security

Singapore
- Cybersecurity Bill

Hong Kong
- Competency Framework on Cybersecurity for the Banking Sector

Kenya
- Central Bank of Kenya - Guidance Note on Cybersecurity

Note 1: List is non-exhaustive

SWIFT Customer Security Programme

"There are only two types of companies: Those that have been hacked and those that will be hacked" Robert S. Mueller, III, Director FBI

"The attacks will continue and get more sophisticated"
Gottfried Leibbrandt, CEO, SWIFT

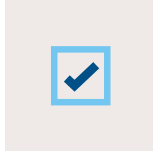
BEST CYBER-SECURITY PROVIDER
Award in 2019

SWIFT recommends 4 lines of defense to mitigate fraud risk

1 – Build Trust

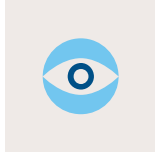
Trust your counterparties through SWIFT's shared **KYC platform** for managing and exchanging standardized Know Your Customer (KYC) data.

Define which counterparties can send them FIN messages through **SWIFT's RMA**



3 – Validate

Payment Controls Reporting profiles your normal payment flows and validates your payment logos against SWIFT data to prevent cyber attackers covering their tracks



2 – Collaborate

Leverage community intelligence on **SWIFT ISAC &** share intelligence on cyber attackers' latest strategies and activities with your community

4 – Protect

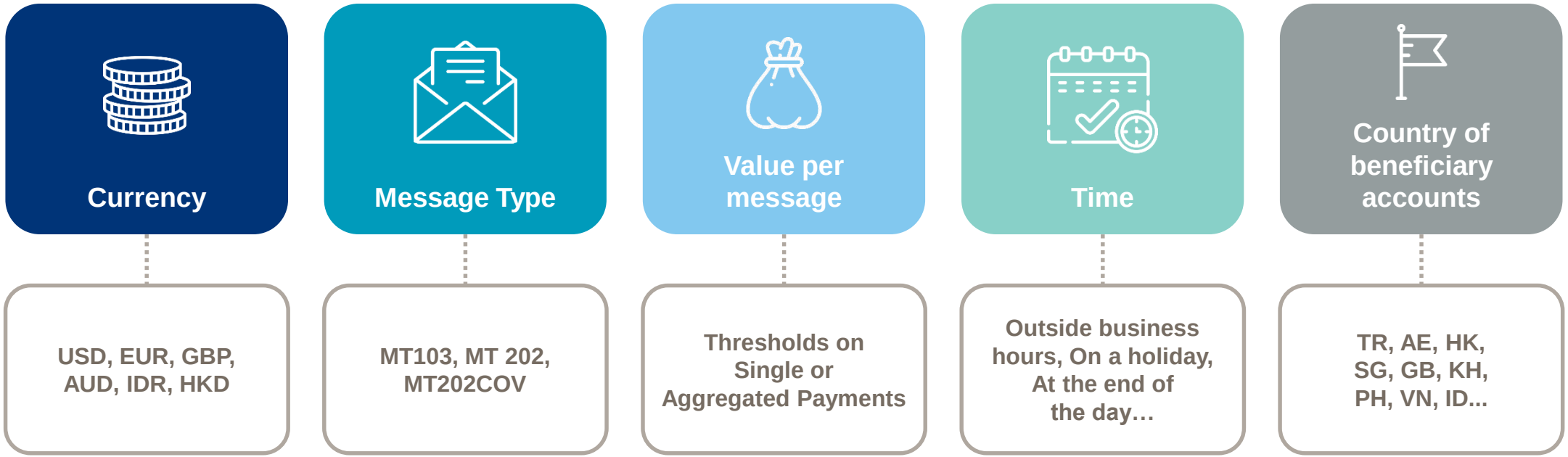
Payment Controls helps you manage your payment policy and **identify unusual or uncharacteristic payment risks** that may be indicative of fraud, and provides an independent snapshot of your SWIFT transaction activity.

Please, INFORM SWIFT!

Register to ISAC portal: https://www2.swift.com/isac/

Dimensions of the fraudulent messages

Attacks are described within the ISAC in different dimensions:



2018-2019 Cyber Trends & Attack Patterns

Available on SWIFT.com

Key Takeaway

Values

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

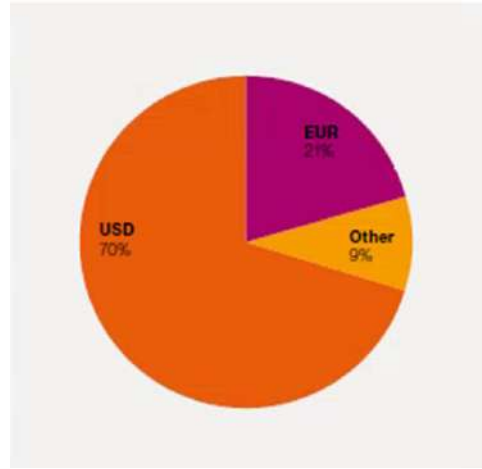
Volumes

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



Key Takeaways

Corridors

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

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

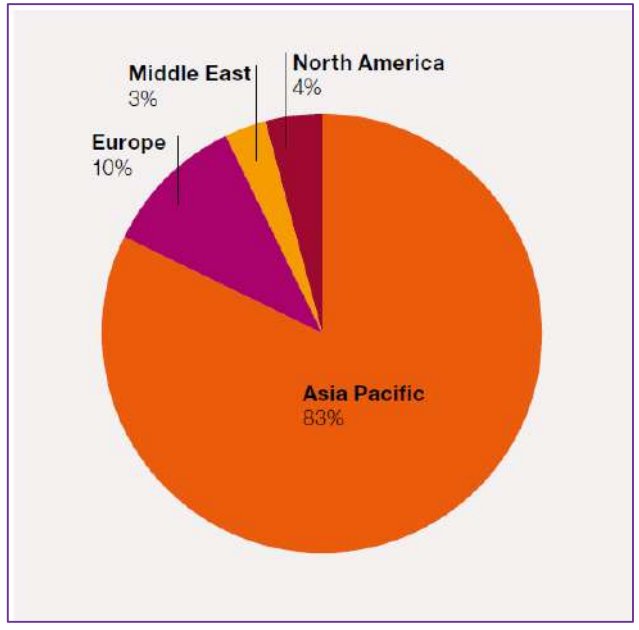
3. Most of the transactions issued were handled by one or two Receiver banks and were intended for the same Beneficiary country.

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.



2019 – More spread in EMEA, more focus in Europe

Symantec – West African Financial Institutions Hit by Wave of Attacks (using similar malware to previous SWIFT attacks) URL - *https://www.symantec.com/blogs/threat-intelligence/african-financial-attacks*

Reuters – Cyber attack on Malta bank tried to transfer cash abroad (Two days after the Bank of Valletta celebrated Safer Internet Day they were forced to pull the plug on their entire online presence, branch and ATM network following a cyber intrusion that involved the attackers attempting to transfer EUR13m to a variety of banks in UK, US, Czech Republic and Hong Kong)

URL - *https://www.reuters.com/article/us-bank-valetta-cyber/cyber-attack-on-malta-bank-tried-to-transfer-cash-abroad-idUSKCN1Q21KZ*

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

Payment Controls | Overview

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 | 2 modules

Module **1**

Reporting- forensic tool

Activity and Risk reporting
Inbound and Outbound
Group and/or Entity reporting

Daily Validation Reports
+
Configuration report (Excel)

Module **2**

Alerting/Blocking in Real-time

Real-time
Outbound
Subscriber-controlled rules

Module 1- Payment Controls Reporting

Support Rule Building

+ Providing data about the traffic your institution sends over the SWIFT network
+ Designed to help you effectively and efficiently **build and maintain rules**.

Validate Activity

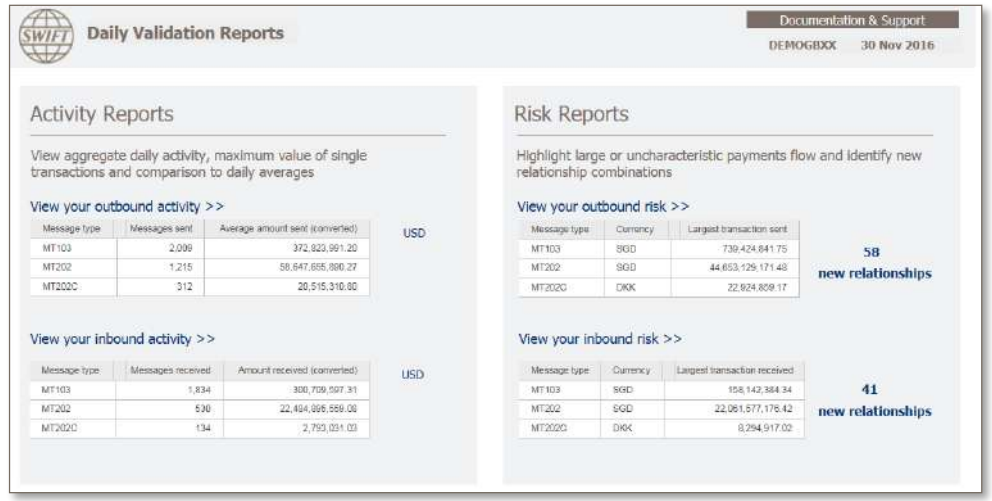
+ **Validate aggregated daily activity and transactions** (reference and value) for a Group or a BIC8 across the payment chain
+ **Daily volume and value totals, maximum value of single transactions and comparisons to 24 months historical profile**

Assess Risks

+ **Assess large or unusual message flows** based on different risk factors (largest transactions, largest aggregates, or deviation with average activity).
+ Identifies new combinations of parties in payment chain
+ highlights transactions sent outside of business hours

Review Behaviours

+ Ensure alignment to Compliance policy



Payment Controls | 2 modules

Module **1**

Reporting- forensic tool

Activity and Risk reporting
Inbound and Outbound
Group and/or Entity reporting

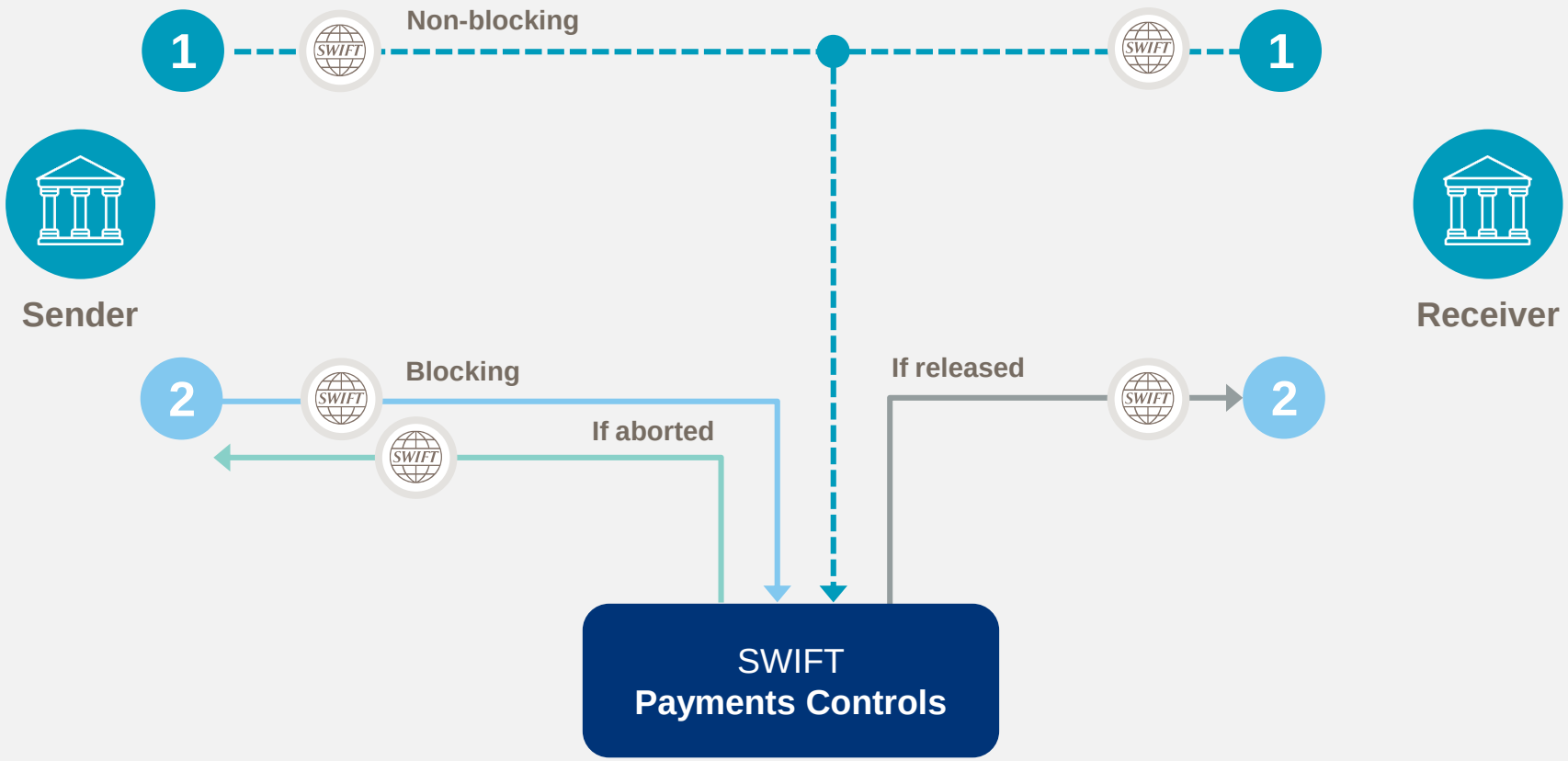
Daily Validation Reports
+
Configuration report (Excel)

Module **2**

Alerting/Blocking in Real-time

Real-time
Outbound
Subscriber-controlled rules

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

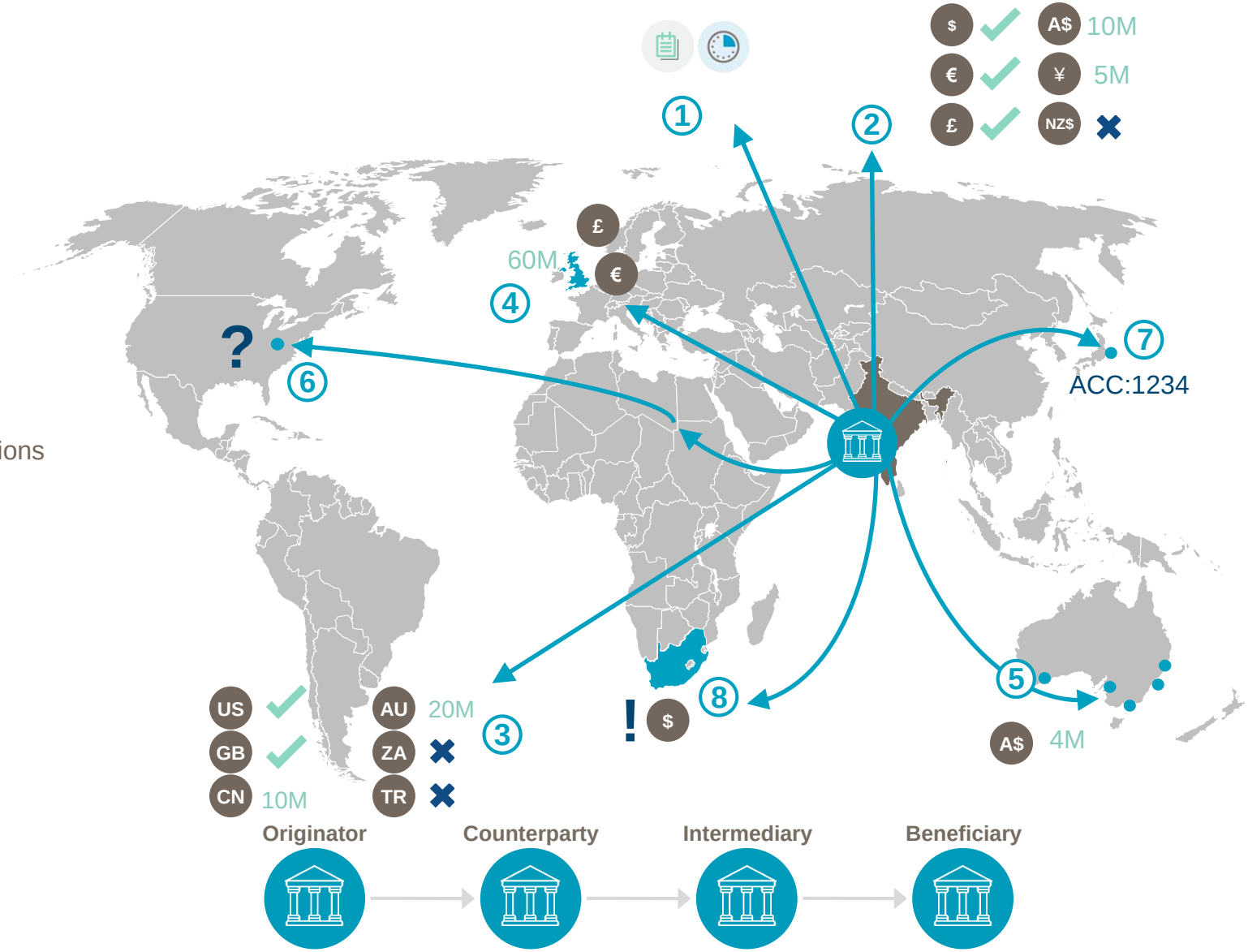
Identify & protect against payment behaviour that is uncharacteristic, based upon past learned behaviour

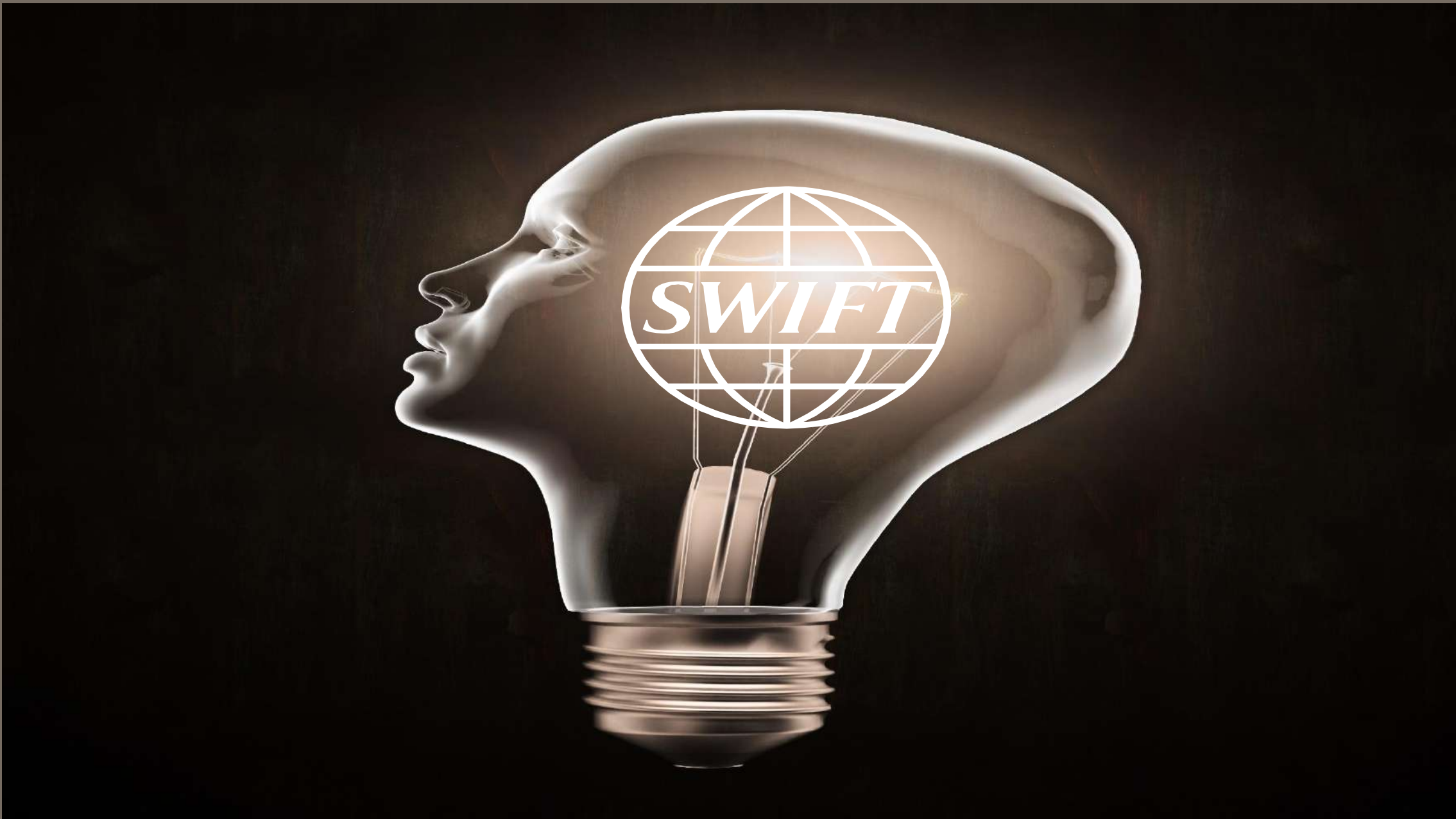
A few examples…

Flexible parameters including:

1. Business hours and days
2. Currency lists, (accept / don't accept) single & aggregate payment limits
3. Country lists, (accept / don't accept) 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




SWIFT