SWIFT Operations Forum Asia Pacific

Financial Crime Compliance – The move to real time & insights from across Asia Pacific

Guy Sheppard, Head of APAC Financial Crime Compliance Initiatives, SWIFT

FCC the APAC story:

Effectiveness vs Efficiency
Trusted Advisors
Fraud
Regtech to Suptech

The global regulatory focus has clearly switched to Asia and Asian regulators have become more active and enforcement-focused…

- **31%** of N.Asia firms surveyed in 2018 under regulator-enforced remediation
  - **288% increase** from 2016 (PWC Financial Observer Report)
- High profile Asian foreign branch "deficiencies";
    - Federal US regulator issues **$110 M** in fines and NY DFS **$395 M** (2017)
    - DFS Part 504 to summarise AML expectations
- **Dormant** now **active enforcement** cultures: MAS and AUSTRAC
  - Post 2016 MAS levied **9 fines** for non-compliance 21M USD and pre 2016……
- **Raising standards: Transparency** and **Effectiveness** of controls
  - HKMA's sanctions filter review and TM assurance to follow…
  - RBI, BNM, MAS, HKMA, JFSA "cyber hygiene" notices
- **Investment in Fintech** eco-system, test sandboxes and "Suptech" preparedness

60 minutes with a GTB: the pace is not sustainable

- The Bank will have made **$210,000** **profit**
- **$41,000** will be **invested back** into FCC
- **114,000** **transactions** processed
- **20,000** cross border payments **screened**
- **1,712** names screened for **PEP** and adverse media
- **30** employees have been through **mandatory AML training**
- **182** **monitoring alerts** completed
- **27** full blown **investigations**
- **2** **SARS** filed – **2** **exits** made

Legalistic versus *effective* compliance

"The challenge that bedevils the industry is the gap between **technical** and **effective compliance**….a firm can have a program that is technically compliant but it is not effective at identifying suspicious activity"

Alan Ketley
Global Head of FCC
Bank of Tokyo Mitsubishi UFJ

Banks – and regulators – are drowning in paperwork. It's expensive, time-consuming and ineffective…

2.16M

Suspicious Activity Reports (SARs) filed in the US in 2017

11%

annual growth in reporting in US, UK, Canada, Hong Kong, Singapore, Australia

80-90%

of SARs have no immediate value to law enforcement

<1%

Less then 1% of criminal funds are frozen or confiscated

Source: **RUSI**

Effectiveness versus Efficiency: a “belief in the theoretical”

- Global Regulatory Compliance (GRC) accounts for **15-20%** of “run the bank” costs
- **Metrics-based** examinations
- Relevance of the SAR/STR regime: US (Greg Baer 2018) and UK Law Commission Report (2019) calls for reform
  - Define “suspicion”; the need for objectivity, standardization and FOCUS
  - Call for use of AI and ML to detect anomalies; different outcomes for different profiles
- The Failure of BPO; GTBs targeting a **30% FTE reduction,** GTBs look to **tech;**
  - Regtech companies raised **$6 billion+** in disclosed equity across **600+** deals…
  - Finextra ‘global banking trends’ saw 70% have **1-4 Fintech solutions** in production
  - **Fraud** and **AML** the top priorities for AI vs UX at only 15%

The FCC profession“..the expectations have increased dramatically from the board, business and the regulator…”

- Remit: from **Processes** to **Programs**
- Role: from legacy KYC Profile to **“Trusted Advisor**”
- Remuneration: a **talent shortage**
  - Tech-savvy, commercial & cross-border experience are key
- A focus on **intelligence** *not* data
- Expansion of the sphere of FCC responsibility;
  - Fraud convergence
  - New missions; wildlife trafficking & “ethical compliance”
  - Change in CTF mission: from Plots to “Lone wolves”,
    - **Al Qaeda** versus **ISIS**
    - **75%** of EU Terror attacks funded <**$10K**

The changing face of Bank fraud …a growth in distance and scope…

“Put your hands in the air and the money in the bag”

“Afternoon ma’am I would like to confirm your account details are up to date…

- Global cost of cyber crime will grow from **$3 Trillion** in **2015** to **$6 Trillion** by **2021**..
- **34%** of breaches involved an insider (Verizon 2019 data breach report)

Cyber…In every case the staff are the weakest and strongest factor at the same time..

"There is a definite **need to educate our network on cyber**, *we also have conversations with central banks…there is* ***clear correlation*** *between those that are engaged versus the disinterested and the* **risk ranking we apply***"*

Richard Williams, Head of Banks & Broker Dealers, Financial Crime, Governance & Advisory,Standard Chartered Bank

- Still a relatively new legislative and reporting discipline
- Move away from system to employee-based attacks
- The key worry is **customer data** being hacked, ransomed or lost
- Increase of attacks on SWIFT connected banks: the "common cold" and new normal
  - Increasingly collaborative approach to cyber heists
  - Change in attack vector: **$10M** to **$250K-$2M** and from *out of hours* to 'plain sight'
  - **83%** of SWIFT payment frauds see the beneficiary account based in SE Asia

Regtech the battle for insight and intelligence NOT data..

"We can and are building **good and bad customer profiles** using AI/ML that will reduce the *'honeymoon'* period of access to bank services while still under-evaluated….if they evolve as I think they will, we will face an **ethical dilemma** of knowing to a high degree of certainty that a customer will not be one we will want in the longer term….how do we explain that to the regulator, to the customer and indeed ourselves?"

Anonymous, Head of Data Science, GTB

- New tech versus old tech versus repurposed tech
- "making your **customers** your (unpaid) **employees"**
- What prevents or slows Regtech adoption?
  - The true price of 'change' : capacity, legacy data etc….
  - Regulatory 'explainability' and acceptance
  - Entrepreneurs as suppliers..
- *Its not Artificial BUT* ***Augmented Intelligence***:
  - Discovering new risk and ML patterns
  - Reducing false positives
  - Increasing automation, data collection versus human analysis

The rise of “Suptech” and the move from “push” to “pull”….

- Machine readable legislation
- A move from reports to data feeds
- The drive for assurance and control transparency
- Investment and promotion of regulatory sandboxes
- Investment in utilities and citizen digitization/biometrics
- Raising standards with thematic reviews
- Data lakes with AI/ML algos and benchmarking bank performance…

But the message is inconsistent; legacy KYC, SAR/STR metrics
“Innovate with caution”

Financial Crime Compliance - SWIFT's role

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 10 services live – More than 6000 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
- Anti-Money Laundering
- Fraud detection

Leveraging SWIFT's and our community's truly distinctive assets

1. Community/reach (11,000 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)

Addressing the complete compliance lifecycle

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

Community driven financial crime compliance utility

The KYC Registry

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

Sanctions Screening

Provides fully-managed, ***securely-hosted screening*** of your customers and transactions against the latest sanctions and PEP lists, with instant alerts of any matches. Provides ***up-to-date sanctions lists*** and capabilities to ***test your own filters.***

Payment Controls

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.

Compliance Analytics

Compliance Analytics portfolio ***pinpoints compliance risks*** and gives a new way to ***monitor your correspondents*** to identify activities indicative of money laundering and ***assess the quality of payment data***.

Cyber resilience & cyber intelligence sharing – how to navigate cybersecurity in the age of digital?

Jeremy Oudkerk, Senior Consultant, Technical & Advisory Services & Partnerships, SWIFT

CYBER
Security
Resilience

“the practice of protecting systems, networks, and programs from digital attacks.”

Cisco

“the skill and the capacity to be robust under conditions of enormous stress and change.”

Diane Coutu

CSP

cyber risk management

Threat management

Vulnerability management

Consequence management

Great, we passed with flying colors !
One less thing to worry about until next year.

Cyber intelligence sharing

If You’re Not Collaborating With Colleagues and Competitors on Cyber Threat Intelligence, Beware: The Bad Guys Are Way Ahead of You

Sherri Ramsay — Cybersecurity Consultant; Former Director of the U.S. National Security Agency / Central Security Service Threat Operations Center

These APT attacks follow the ‘cyber kill chain’

1 month to 2 years	In customers’ environment
0 to 2 weeks	In customers’ messaging interface
0 to 6 hours	Sending fraudulent messages

THE CYBER KILL CHAIN® LOCKHEED MARTIN

“When it comes to Cyber Security, we are all in it together”

Jeremy Oudkerk, SWIFT

“We must work together like the bad guys do—only better”

Anonymous

Cyber intelligence sharing

Your Community

SWIFT has deepened its cyber security forensics capabilities, providing **unique intelligence on customer security-related events.** This information is disseminated to the community in an anonymized manner.

You
Secure and Protect
SWIFT Tools
Customer Security Controls Framework

Your Counterparts
Prevent and Detect
Transaction Pattern Detection – RMA, DVR and Payment Controls

Your Community
Intelligence Sharing
- CSI Forensics
- Security Notifications
- SWIFT ISAC Portal
- Emergency Notification
- STIX/TAXII

Customer Security Intelligence - Function

Information sharing: moving towards SWIFT-ISAC

ISAC: Information Sharing and Analysis Centre

- Live since May 2016
  - Contains reports (“Security bulletins”) with
    - Modus Operandi of different actors (also called TTP: Tactics, Techniques and Procedures)
    - Specific Indicators of Compromise (IOC) related to malware, IP-addresses,…
    - more generic updates on CSP attestation and Mandatory security updates
  - Contains a bulletin with machine digestible information

Security notification mail

- Subscription to ‘newsletter’
- All registered www.swift.com users can subscribe

Information sharing: moving towards SWIFT-ISAC v2

ISACv2 (deployed February 2018):

- Onboarding of non-SWIFT customers (Law enforcement, Cyber Security vendors, ISAC's and CERT's)
- Automated feeds for full integration with existing tools at customer side. protocol in STIX format (industry

SWIFT-ISACv2 | How do you get access to automated feed (STIX/TAXII) ?

- SWIFT whitelists the provided IP address
- SWIFT provides the customer with:
  - Username
  - Password

Where we are now | intelligence sharing

Security Notifications

12,000
unique users

6500
unique BICs

SWIFT ISAC Access (rolling year)

19k
accesses

5400
unique users

27%
of BIC population

200
countries

Available as STIX/TAXII feed

SWIFT ISAC: Filenames; Filehashes; IP addresses; Domains; Ports; Processes; YARA Rules; MO …

Modification Date	Title	Information Type	Attribution	TLP	Tracking ID	Attachment	Favorite
2019-09-12	Information about malicious domains impersonating SWIFT Updated	IOC		TLP:GREEN	10076	Yes	☆
2019-09-12	IOCs in machine-digestible format Updated	IOC		TLP:AMBER	10001	Yes	☆
2019-09-04	Phishing e-mails impersonating SWIFT or referring to SWIFT transactions - Q3 2019 Updated	IOC		TLP:GREEN	10099	No	☆
2019-07-15	CSCF 2020	Security Information		TLP:GREEN	10098	No	☆
2019-07-15	SWIFT ISAC automated feed - Frequently Asked Questions SWIFT ISAC	General Information		TLP:AMBER	10073	Yes	☆
2019-05-20	Phishing e-mails impersonating SWIFT or referring to SWIFT	IOC		TLP:GREEN	10097	No	☆

Share

Where we are now | intelligence sharing

CSP

Cyberattacks on SWIFT customers continues

For 2019, the rate of new, confirmed customer cases is similar to 2018

Customer Security Programme

Launched in 2016 in response to the attack on Bangladesh Bank, CSP is a multi-year, multi-facetted initiative

CSP aims to transform the institutional financial services ecosystem by raising the bar of cybersecurity hygiene, reducing the risk of cyberattacks and minimising the impact of fraudulent transactions

Where we are now | controls

Improve cybersecurity hygiene

CSP Security Controls		
Secure Your Environment	1.	Restrict Internet access
	2.	Segregate critical systems from general IT environment
	3.	Reduce attack surface and vulnerabilities
	4.	Physically secure the environment
Know and Limit Access	5.	Prevent compromise of credentials
	6.	Manage identities and segregate privileges
Detect and Respond	7.	Detect anomalous activity to system or transaction records
	8.	Plan for incident response and information sharing

Where we are now | attestation

Community is engaged

94%
Attestation

>99%
Traffic

Where we are now | controls evolution

Raising the bar

2017

2017
- 27 Controls
- 16 Mandatory +11 Advisory
- Self-Attestation by 31 Dec17

2018

2018
- 27 Controls
- 16 Mandatory +11 Advisory
- Compliance by 31 Dec18

2019

2019
- 29 Controls
- 19 Mandatory + 10 Advisory
- Compliance by 31 Dec19

2020

2020
- 31 Controls
- 21 Mandatory + 10 Advisory
- Compliance by 31 Dec20

Where we are now | assurance

Assessment Type	Selection Criteria	Assessor	Timeline			
			2017	2018	2019	2020 and beyond
❶ **User-Initiated Assessment**	Voluntary - Customer Initiated	Internal or external				
❷ **Community-Standard Assessment**	Mandated - All Users	Internal or external				
❸ **SWIFT-Mandated Assessment**	Mandated - Sampled Customers Driven by QA Analysis	External only				

Where we are now | counterparty risk management

Establish a **governance** model

Adopt cybersecurity risk **countermeasures**

Establish a cybersecurity **risk management** framework

Incorporate cybersecurity **attestation data** from SWIFT counterparties

Customers do not operate in a vacuum

Where we are now | payments control service

Fraud detection

'In-flight' transaction monitoring on 'sent' payments and identifies activity that is out-of-policy or indicative of fraud

PCS Tuning Parameters

- **Business Calendars,** normal hours and non-business days
- **Currency** whitelist / blacklists, single and aggregate payment limits
- **Country** whitelist / blacklists, single and aggregate payment limits
- **Thresholds** for country, currency, single entity or group combinations
- **New Institutions**: Identify payments with new participants or chains
- **Suspicious Accounts:** institution black list of high risk account numbers

Current roadmap focuses on controls, assurance and risk

Call to action for SWIFT customers

1. Stay up to date with SWIFT software releases
2. Sign up for Security Notifications and use of the SWIFT ISAC information sharing portal or STIX/TAXII feeds
3. Consume and utilise attestation data for counterparty risk management
4. Consider SWIFT's anti-fraud tools (Payment Controls, Daily Validation Reports, RMA clean-ups, etc.)
5. Always inform SWIFT immediately if you suspect a cyber-attack on your SWIFT-related infrastructure
6. Ensure that you fully comply with all the mandatory security controls and attest by end December

Questions

Improving the security of payments in Asia Pacific

Guy Sheppard, Head of APAC Financial Crime Compliance Initiatives, SWIFT

Three years on from Bangladesh

Tackling fraud with SWIFT Payment Controls

World Economic Forum ranks ‘cyberattacks’ as a top global risk

Source: 2018 WEF survey spanning 684 respondents which assessed [likelihood] and [impact] of each risk on a scale of 1 to 5 [very unlikely / minimal impact] to [very likely / catastrophic]

“Financial institutions and payment infrastructures are the new targets

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

Staying ahead of Cyber Crime UK Finance – April 2018

Convergence of compliance & fraud prevention

43%

of compliance teams are now involved in cyber resilience*

"AML needs to keep up with new monetization and cash out channels to allow fast blocking and or funds recovery"

Staying ahead of Cyber Crime UK Finance – April 2018

*Survey: Cost of Compliance 2018, Thomson Reuters

The changing face of Bank fraud …a growth in distance and scope…

“Put your hands in the air and the money in the bag”

“Afternoon ma’am I would like to confirm your account details are up to date…

- Global cost of cyber crime will grow from **$3 Trillion** in **2015** to **$6 Trillion** by **2021**..
- **34%** of breaches involved an insider (Verizon 2019 data breach report)

Regulatory focus on cyber security | RBI guidelines

Structure of RBI

Guidelines on Cyber Security Framework

RBI Guidelines on Cyber Security framework focus on the following three areas:

01. Cyber Security and Resilience
02. Cyber Security Operations Centre (C-SOC)
03. Cyber Security Incident Reporting (CSIR)

The Cyber Security Framework for bank widely covers the follows domains:

Cyber Security Framework

Cyber Security Policy	Cyber Security Strategy	Continuous Surveillance	**Annex 2 – Cyber Security Operation Centre (C-SOC)**
Risk / Gap Assessment	IT Architecture		
Network and Database Security	Cyber Security Policy		
Cyber Crisis Management Plan	Cyber Security Preparedness Indicators	Reporting Cyber Incidents	**Annex 3 – Cyber Security Incident Reporting (CSIR)**
Organization Structure	Cyber Security Awareness		

Annex 1 – Baseline Cyber Security and Resilience Requirements

Detailed Requirements of Cyber Security Framework

The detailed requirements for each of the Annexures of Cyber Security Framework are as follows:

Annex 1 – Baseline Cyber Security and Resilience Requirements

Inventory Management of Business IT Assets	Preventing execution of unauthorized software	Environmental Controls	Network Management and Security	Secure Configuration
Application Security Life Cycle (ASLC)	Patch/Vulnerability & Change Management	User Access Control / Management	Authentication Framework for Customers	Secure mail and messaging systems
Vendor Risk Management	Removable Media	Advanced Real-time Threat Defense and Management	Anti-Phishing	Data Leak prevention strategy
Maintenance, Monitoring, and Analysis of Audit Logs	Audit Log settings	Vulnerability assessment and Penetration Test and Red Team Exercises	Incident Response & Management	Risk based transaction monitoring
Metrics	Forensics	User / Employee/ Management Awareness	Customer Education and Awareness	

Annex 2 – Cyber Security Operation Centre (C-SOC)

Cyber crime is lucrative as it is damaging… the "iceberg effect"

- Total APAC economic loss to cyber crime **$1.745 Trillion**
- **This is 7% of Asia's GDP**
- N. Korea generated **$2.77 Billion** via "widespread & increasingly sophisticated" cyber attacks (UN)

Cybersecurity threats to cost businesses in Malaysia **$12.2 billion**

= **4%** of 2017 **national GDP**

The Total economic impact of Cyber attacks:

$30 million
(av. loss for a large company)

- **'Direct'** — **$3.4 Million** (tip of the iceberg)
- **'Indirect'** — **$9.7 Million** (loss of customers/ reputational damage)
- **'Induced'** — **$17.2 Million** (amplified impacts across eco-system; loss of jobs/ growth)

Close to **7** in **10** had **job losses** due to security incidents

1 in 2 organisations has **either experienced a cyber attack** or is unsure if they have a security incident

Source: Dr Haji Amirudin Bin Abdul Wahab, CEO CyberSecurity Malaysia A&C 2019 KL

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
Amounts
Reconnaissance
Timing
Message Types
Currencies
Beneficiaries
Conclusion

Beneficiaries

Beneficiary or “mule” accounts are critical for attackers’ ability to extract funds from the financial system – without these compromised accounts, they would be unable to materialise any of the fraudulent funds. Gaining an understanding of 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 provides interesting data on the Beneficiary accounts. SWIFT was able to extract Beneficiary country information from the fraudulent messages sent in 2018 information which revealed some differences in pay-out techniques. What was most notable, however, was the concentration of the Beneficiary banks in Asia Pacific: 83% of all fraudulent transactions had a beneficiary account in East and South East Asia. The remaining 17% 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 2018.

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 financial crime compliance portfolio and an important element in the CSP to strengthen the global financial community’s defences against cyber threats as the frequency and speed of payments increases.

Daily Validation Report

The Daily Validation Report tool helps to mitigate the risk of lost records by providing daily activity and risk reporting of your previous day’s SWIFT transactions. Activity reporting allows institutions to verify their payment messages against SWIFT’s own record – which is critical if customer environments are compromised. Risk reporting allows institutions to focus on changes in activity that may indicate significant payment risks provides aggregated transaction totals by counterparty, and flags new correspondent relationships.

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 online 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 illicit or unusual message flows.

Using the tool, customers can define their own monitoring policy, controlling their parameters to enable timely detection and prevention of out-of-policy or uncharacteristic 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 protect payment operations. Doing this reduces the risk of fraud and gives operations teams tighter overall control.

Introduction
Targets
Amounts
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 Attestation” tool as the central application for the submission of self-attestation data. The KYC-SA 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 attestation and compliance with the controls, as institutions seek to demonstrate their cyber security to their counterparties.

Cyber security risk introduced by counterparties needs to be managed alongside other types of risk. Many institutions are therefore already integrating cyber risk assessments into their existing risk processes by incorporating the assessment of counterparties’ CSCF attestation data into their risk management and business decision-making processes.

As outlined in the recently published guideline ‘Assessing 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 correlating known indicators to support risk-driven decisions;
- Processing this data and transforming it into a weighted, risk based assessment, typically shown as a numeric score or a red-amber-green indication;
- Adopting suitable countermeasures to mitigate or “treat” the risks.

To support the risk assessment of incoming transactions from counterparties, institutions should assess how incoming transactions from counterparties correlate against the profile of existing incidents, e.g. country/region of sending counterparty, country/region of end beneficiary, transaction type, transaction currency, transaction value, transaction timing and frequency.

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, seek security-enhancing innovations in our own products and services, and work to increase the scope and quality of threat intelligence sharing.

Our information sharing initiative has contributed to significant 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 supplement the fraud controls that financial institutions would already have in place.

The industry should continuously increase the strength and diversity of its defences and ensure it understands the nature of the changing threat. This means being proactive in limiting criminal opportunities, linked to systems and business practices, by means of ensuring proper protected ness and understanding counterparty cyber risk.

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

Available on **SWIFT.com**

Cyber…In every case the staff are the weakest and strongest factor at the same time..

"There is a definite **need to educate our network on cyber**, *we also have conversations with central banks…there is* ***clear correlation*** *between those that are engaged versus the disinterested and the* **risk ranking we apply***"*

Richard Williams, Head of Banks & Broker Dealers, Financial Crime, Governance & Advisory,Standard Chartered Bank

SingHealth Defining Tomorrow's Medicine MAERSK SWIFT

- Still a relatively new legislative and reporting discipline
- Move away from system to employee-based attacks
- The key worry is **customer data** being hacked, ransomed or lost
- Increase of attacks on SWIFT connected banks: the "common cold" and new normal
  - Increasingly collaborative approach to cyber heists
  - Change in attack vector: **$10M** to **$250K-$2M** and from *out of hours* to 'plain sight'
  - **83%** of SWIFT payment frauds see the beneficiary account based in SE Asia
  - Use of dormant RMAs or underused corridors

SWIFT

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

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

Dimensions of the fraudulent messages

Attacks are described within the ISAC in different dimensions:

Currency	Message Type	Value per message	Time	Country of beneficiary accounts
USD, EUR, GBP, AUD, IDR, HKD	MT103, MT 202, MT202COV	Thresholds on Single or Aggregated Payments	Outside business hours, On a holiday, At the end of the day…	TR, AE, HK, SG, GB, KH, PH, VN, ID...

Payment Controls Alerting

Message Type

Country of beneficiary accounts

Currency

Value per message

Message Type

Time

Payment Controls – Create Rules

Screening Utility TEST | Alerts | Payment Controls | Administration | roy-belchamber

Configuration

Back to overview

Ruleset
SWIFTLab Demo Ruleset Edit title and description

Created on	08 Oct 2018 08:12 GMT	Owning BU	SWIFTLab	Current active date	14 Oct 2018 19:17 GMT	Messaging BIC(s)
Last updated on	14 Oct 2018 19:18 GMT	Last updated by	roy-belchamber	Current draft date	14 Oct 2018 19:18 GMT	

Message count (1) | Single payment (3) | Amount aggregation (1) | Account monitoring (1) | Business calendar (1) | New scenario (1)

Live rules (3)

State	Rule action	Expiry action	My role	Ordering	Counterpart	Beneficiary	Currency
	Blocking	Abort	Ordering	Me	Any	Any	NOT_IN USD, EUR, GBP, CHF, MXN
	Non Blocking		Ordering	Me	Any	Any	Any
	Non Blocking		Ordering	Me	Any	NOT_IN GB, US, ES, CN, HK, NL, CA, DE, CH, ZA, FR, SE, SG, JP, AU, DK, IT, LU, NZ, IE, AT (COUNTRY)	Any

Test rules (0)

Create 'Business calendar' rule

1. General information

Rule title * Business operating days
23/100

Rule description Rule for our standard business day and hours
44/256

Rule action * Non-Blocking
When the rule is triggered, a non-blocking, acknowledgement-only hit will be generated

2. Define regular working hours

	Applicable from *	Applicable to *
	2017-01-01	2017-12-31

	Working day start	Working day end
Monday	03 00	22 00
Tuesday	06 00	22 00
Wednesday	06 00	22 00
Thursday	06 00	22 00
Friday	06 00	22 00
Saturday	00 00	00 00
Sunday	00 00	00 00

3. Set optional overrides for specific dates

	Start date/time	End date/time
2017-12-25	08 00	12 00

Cancel | Save rule

Payment Controls – View the Alerts

Payment Controls – Remediate Each Alert

Question and Answer

STIJN DE CLERCQ | Product Management AMH
JACQUES VAN LEYNSEELE | Professional Services AMH

THE FUTURE IN FINANCIAL MESSAGING - AMH

SOFA 2019

Warming up.

HAVE YOU HEARD OF AMH?

DID YOU KNOW ABOUT MULTI-NETWORK SUPPORT?

DID YOU KNOW AMH IS CLOUD AWARE?

SWIFT's integration & interface offering

Integration and interface products for today's financial market needs

Key Performance Figures

5+ million

Sent and received FIN messages daily

10+ GB

Sent and received FileAct transfers daily

1500

Concurrent users

1.26 min

Max time to recover in case of fallback

Up to 2100

Transactions per second throughput

100 milliseconds

In 99th percentile one-leg processing time in STP

Alliance Messaging Hub

A Highly customizable platform.

TCO REDUCTION

TCO REDUCTION

Key Benefits for IT and Operations

3 to 8 TCO savings factor

Horizontal & Vertical scalability

Reduced annual recurring effort

Maximize latest hardware

Aggregated & digressive volume based price

SECURITY

SECURITY

AMH offers the highest level of security.

Advanced User Profiles

DB Sealing

PS Security Review

Application server shielding and hardening

CSP

Use Case PS

SWIFT INFRASTRUCTURE (CSP) SECURITY REVIEW

RESILIENT & SCALABLE

RESILIENT & SCALABLE

Processing a large volume of messages, AMH offers high levels of availability, high performance, flexible flows and a modular structure.

Robust

Performance

Vertical and Horizontal scalability

Flexible Flows

Modular

Modularity: unparalleled flexibility to scale

Benefits:

- Cope with business growth
- Segregation of flows to meet performance SLAs by vertical scalability
- Adjust to the environment changes
- Dedicated service per instance
- Segregation of networks
- Agility to respond to business
- Central flow monitoring
- High performance through horizontal scalability (multiple instances with common database or individual database)
- Dedicate resources to meet business SLAs (priority)

ARCHITECTURE & RESILIENCE

Single Instance active-passive setup.

SINGLE INSTANCE / DUAL SITE

ARCHITECTURE & RESILIENCE

Dual active setup.

DUAL INSTANCE / DUAL SITE

ARCHITECTURE & RESILIENCE

Dual active setup with AMH Workbench.

- STP lane:
Flow control, routing, distribution and communications handling (optional).

- Global end-user workbench:
Single view for exception handling, message search and monitoring.

DUAL INSTANCE / DUAL SITE

AMH WORKBENCH

Scaling option to leave full processing power to STP and separated environment for users.

Benefits

- Consolidated view of exceptions (when multiple STP)
- 4-eye validation possible for extra security
- Tracking of manually handled messages in history and logs
- User defined searches for management of messages

INSTANT & MULTI-NETWORK

INSTANT & MULTI-NETWORK

AMH Messaging Hub
for multiple networks.

SWIFT NETWORK

MULTI-NETWORK

AMH INSTANT FOR INSTANT PAYMENTS

MULTI-NETWORK

- Corporate
- Third Party Payment Service Provider
- Financial Institution
- Market Infrastructure
- Shared Business Services Providers

SWIFT network

Internal applications & Shared services

Business applications

Financial networks

- ✓ euroSIC/SIC
- ✓ SECOM
- ✓ TCH RTP & CHIPS
- ✓ FedWire Funds
- ✓ RT1 and TIPS
- ✓ HK FPS (PS)
- ✓ MY RPP (PS)

AMH User Interface

Workbench

Control Centre

AMH Server

Connectivity

- Integration for SWIFT network connectors
- Multi-network
- Intra-Company communication
- Crypto services

Orchestration

Workflow management

Message Handling

Transformation
Validation
Enrichment

External Database

Message information & audit

Operational data

Message Formats libraries

Message Mapping

Reference Data

INSTANT PAYMENTS

Introduces a **new** instant messaging protocol (SWIFTNet **Instant**)

Re-uses the existing SWIFTNet **connectivity** and **security** infrastructure

Re-uses SWIFTNet **FileAct** and **Browse**

*existing infrastructure (if AMH this infrastructure can also form the basis of the orchestration hub)

SWIFT MI

ISO20022

Delivering Common functionality in a flexible ISO 20022 world.

FIN Alignment

- Granular RMA Support on InterAct
- Address book validation for CBPR+
- Copy Mechanism changes support
- Tbc : Pretty print & Amount limits management

Usage Guidelines Support

- STP validation supporting the specific CBPR+ and ESMIG T2 Market Practices
- Leveraging SWIFT Standards expertise and Artefacts for Validation and Translation

ISO 20022 gpi support

- Single UETR payments GUI
- Generation of UETR for ISO 20022 payment messages

Local Translation & Orchestration

- Building blocs to facilitate both ways translation
- Support CBPR+ Multi-formats MX and Local Translation
- Routing rules and Fields extraction (or equivalent) enhancements

Deployment Agility

- Protocol specifics (signature, IA/FA selection, (De)compression, (De)bulking,…) management
- Integrated in specific T2 and T2S ESMIG subflows
- FileAct file retrieval

TOOLS

TOOLS

TRANS-
FORMATION
WORKFLOW
SYSTEM
MONITORING
LONG
TIME
ARCHIVE
AMH WORKBENCH

System Monitoring

Enhancing the corporate experience in cross-border payments

Benefits

- Improve system visibility
- Up to date status information
- Real time information
- Clear graphical or tabular view
- Optimized interactions with system
- Optimized searching
- Alerting with clear information
- Fast issue resolution
- Colour code status
- Hierarchy of components
- Several views: general, SAG, FIN, SIX, channel
- Dashboard capabilities

AMH TRANSLATOR

Benefits

- With SWIFT Translator, defining, mapping and validating messages from any format to ISO 20022 or MT becomes a breeze.
- SWIFT Translator eases standards migration and customer onboarding projects, while simplifying formats translation, mapping and validation.

AMH WORKFLOW

Business Process Management

Benefits

AMH contains a Business Process Management engine (BPM)

- Industry standards compliant (XPDL)
- Both STP and manual activities interaction
- Native integration of SOA services

Reference workflows are included

- Rapid time to market
- Tailored towards customer requirements

Alliance Warehouse

Easily store and search all your transaction data.

FUTURE PROOF

FUTURE PROOF

Architectural and
Technology roadmap

COMPONENT BASED ARCHITECTURE

AMH Roadmap includes a future proof service oriented architecture.

[Tentative]

Monolithic Architecture

Standalone Components

[Tentative]

COMPONENT BASED ARCHITECTURE

AMH Roadmap includes a future proof service oriented architecture.

[Tentative]

EXTENSIBILITY FRAMEWORK

Allow easy development and safe integration of custom code and add-on services.

[Tentative]

CLOUD AWARE

We are expanding options for customers moving to the cloud.

CLOUD CONNECT

- Enable hosted HSM/VPN connectivity to SWIFT in Public Cloud.
- 2020 launch with demand based support for various mega-cloud providers.

AMH CLOUD AWARE

- AMH runs in Public Cloud.
- Evolution to cloud native architecture.
- Cloud easy install on AMH Roadmap.

SWIFT Public Cloud offering:

[Tentative]

API ROADMAP

APIs are touching every facet of the financial sector.

API proxy

- gpi Connector

API consumer (future)

- gpi API (Roadmap)
- Transaction Sanctions Screening API

API provider (future)

- Message data API
- Reference data API

[Tentative]

UX

Roadmap includes UX improvements on AMH.

User Experience becomes part of our DNA and it drives and defines how our existing products evolve and how new products are designed and build.

UX +

Designing the Alliance product portfolio with a carefully balanced amount of features in line with customer and user needs.

Intuitive, familiar and easy to learn: users will not have to read extensive documentation or attend lengthy training courses to use our platform.

Our platform will allow users to do their work more efficiently, saving them precious time and enabling them to do more.

[Tentative]

UX

Roadmap includes UX improvements on AMH being more intuitive, familiar and easy to use.

Future UI

AMH ROADMAP

AMH roadmap principles: 4 streams

Evolution of the AMH “core” platform through constant modernization and adoption of latest technology.	CORE
Further extension of AMH feature library, evolution into multi-network packages.	NETWORKS
Readiness for evolving business initiatives such as GPI, MI initiatives, ISO20022, …	INITIATIVES
Continuous implementation of customer requirements.	CUSTOMER

[Prototyping stage]

CORE

Technology

2019

Shielded Database Pilot

2019-2021

POC's Prototypes Demo's

2022-2023

New "Open" Platform

"Modernize AMH to an easy to operate component-based platform with a more open architecture"

UX - Enhanced look & feel

NETWORKS

SWIFT

2019

Fedwire Funds, TCH CHIPS

2019

Enhanced Formats mgt

2020 TBD

UK Fedwire, ISO20022

"Maximize the value of AMH as multi-network hub by plugging in more networks & enhancing the platform"

Watch trends

Such as …

Big currencies

Networks undergoing renewal (ISO20022)

Avoid legacy

STP / real-time focus

Plug-in more networks

By …

Providing an AMH solution package

Enhancing the platform to support a custom project

Explore partnership

Either …

SWIFT directly engaging with network provider or with a partner

SWIFT working with the bank

The bank running a project, leveraging the AMH platform

INITIATIVES

SWIFT & MIs

2019 - 2020

Integration with API Gateway

2019 - 2020

Additional 20022 features

2021

ESMIG & HK CHATS

“Enable our customers on latest SWIFT & MI Initiatives, leveraging the real-time orchestration power of AMH”

CSP	ISO20022	SWIFTNet	API@SWIFT	gpi
Continue enhancing AMH to facilitate CSP compliance for our customers	Enhance AMH for better ISO20022 support, provide solution packages, ESMIG support (incl. T2)	Align with SWIFTNet and SWIFTNet Instant evolution	Orchestration from and to AMH towards the new SWIFT API platform	Orchestration from and to AMH towards the new SWIFT API platform, gpi on ISO20022

CUSTOMER

Agility

2019

New backlog mgt

2019

Increase customer interaction

2020-2023

Extensibility framework

“Bring value to our customer’s specific business needs while enriching AMH and offering extension points”

New backlog management process

Increase customer touchpoints

Extensibility Framework

Current – SIL next to AMH

Mid-term – increase SIL & AMH co-existence

Longer-term – foresee Extensibility Framework in the future Component Based architecture

www.swift.com