Equipping the community

SWIFT's financial crime compliance portfolio expands in response to evolving industry needs.

Across its four-day programme, the Sibos 2017 compliance stream echoed the need for change felt by many of the industry's financial crime compliance (FCC) professionals. Speakers urged a more coordinated approach across related disciplines, greater information-sharing and an increased use of technology to facilitate value-added tasks, supporting risk-based strategies and reducing duplication of effort.

This desire to improve the effectiveness and efficiency of banks' FCC efforts was also reflected throughout a diverse programme of SWIFT Auditorium and SWIFTLab sessions. These highlighted the increasing scope of SWIFT's FCC product suite, and its synergies with other strategic initiatives, notably SWIFT's Customer Service Programme (CSP), which supports users' cyber-security capabilities.

Two key announcements at Sibos also underlined SWIFT's ongoing commitment to deliver solutions that address the needs of all of its members. SWIFT has aligned The KYC Registry with the Wolfsberg Group's recently revised Correspondent Banking Due Diligence Questionnaire in an effort to drive global due diligence standards and enable Registry users to save time and costs associated with repetitive data collection.

And in the area of anti-money laundering (AML) checks, SWIFT has expanded its Name Screening service, targeting the need for smaller firms and institutions in emerging markets to prevent financial crime. Since Name Screening can be easily customised to address local regulatory requirements and institutional risk policies, it can support the compliance needs across the payments industry.

On Monday, discussion centred on the use of SWIFT messaging data to support correspondent banks' due diligence processes. SWIFT launched Compliance Analytics in 2014 to enhance the effectiveness of banks' sanctions and KYC programmes. According to AML managing director Andy Hofmann, Compliance Analytics has helped Canada's BMO Financial Group tackle specific issues – e.g. ensuring adherence to country sanctions imposed by the US – while also improving efficiency, increasing transparency and reducing risk across its correspondent banking relationships.

As well as identifying dormant relationships, Compliance Analytics highlighted exposures to particular countries and institutions, prompting the firm to reassess or revisit existing relationships. "Compliance Analytics helps us identify problems with our customers before other banks notice them," said Hofmann, noting also unexpected benefits to relationship managers seeking new sales opportunities.

> **"Compliance Analytics helps us identify problems with our customers before other banks notice them.**
>
> Andy Hofmann, BMO Financial Group

SWIFT has now introduced a new module – Correspondent Monitoring – to help banks address money-laundering risks within correspondent banking networks. Correspondent Monitoring allows banks to analyse their SWIFT message traffic to uncover unusual activity patterns and risk exposures within their correspondent banking networks. For example, a user can find out whether it was in receipt of transactions originating in a country considered high risk or subject to sanctions via correspondents operating in a low-risk jurisdiction. Further, the tool's rules engine can be set to detect and report specific high-risk activity patterns on an ongoing basis.

Correspondent Monitoring was developed specifically to help banks untangle the complexity of correspondent banking transaction chains. Hendrik Ooghe, SWIFT FCC product manager, explained: "Bank A needs to understand whether activities by its counterparty, Bank B, might present hidden risks. For example, is Bank B receiving or sending payments involving high-risk jurisdictions? Correspondent Monitoring helps you understand what kind of flows your correspondent is involved with, so you can take appropriate compliance and risk-control measures."

Spotlight on fraud

On Thursday the spotlight turned to the fight against fraud, where SWIFT is providing users with controls and insights that will bolster banks' own resources and support SWIFT CSP's cyber-security objectives.

As explained by Delphine Masquelier, product manager for financial crime intelligence, SWIFT's Daily Validation Reports provide users with an independent means of checking whether their transaction systems have been altered by cyber-criminals. Users access a SWIFT report to check against their own records for discrepancies that could indicate their defences have been breached. As well as making daily comparisons to identify fraudulent activity, the service also allows users to understand trends over time, facilitating comparisons with traffic volumes and values in prior periods to potentially flag suspicious activity. "The risk reports can focus analysis on specific risk factors, such as high-value or unusual payment types, new combinations of parties in a payment chain, or execution outside of normal business hours," Masquelier added.

Payment Controls will build on these capabilities when launched in 2018, providing

continued on page 4

continued from page 3

real-time in-network message monitoring of transaction flows, enabling subscribed banks to alert or block payment instructions identified in breach of policy or outside of expectations. Roy Belchamber, product manager at SWIFT, emphasised the bank configurability and flexibility of the service, which can be adapted to reflect evolving risk priorities and business requirements.

Set alongside presentations on individual products and services, a Tuesday session provided 'high-level' context, emphasising the depth of SWIFT's commitment to meeting the needs of users across the payments and securities sectors. Luc Meurant, head of FCC at SWIFT, explained the need for the cooperative to continue to expand its support for users' compliance needs through utility-based solutions that address increasing operational complexity, regulatory scrutiny and individual liability, and then outlined the role of a new Senior Advisory Group for compliance.

Evolving from the existing Sanctions Advisory Group, the new broader body will be tasked to ensure SWIFT product development priorities remain closely targeted on evolving client needs. It is led by two SWIFT board members: Fabrice Denèle (advisory group chair), member of executive committee at Natixis Payment Solutions, and Mark Gem (vice-chair), head of compliance at Clearstream.

Speaking in his SWIFT role, Denèle said it was important for the cooperative to broaden the scope and the membership of its advisory group to encompass the widening range of FCC challenges and to gain input across multiple geographies and product areas. Gem pointed out the parallels between the compliance challenges facing payments banks and those faced by the securities services sector – e.g. complex transaction chains that obscure originators and beneficiaries – and noted the need to leverage expertise, experience and technology solutions across traditional silos.

The optimisation of existing and proven assets through application of technology innovation can be a key element of the industry's arrival at a more efficient and effective approach to compliance according to Paul Taylor, head of financial crime compliance product marketing, SWIFT. "SWIFT continues to be a driving force behind industry change in compliance. By taking an innovative approach to strengthening our product suite we deliver solutions that address the needs of our community." □

"Risk reports can focus analysis on specific risk factors.

Delphine Masquelier, SWIFT

Community spirit

Innovation, compliance and security topped the agenda as SWIFT's chairman, CEO and senior executives provided an update of the cooperative's strategic priorities at the annual SWIFT Chairpersons Meeting on Sunday 15th September.