Sibos Issues

2016

The official daily newspaper of Sibos 2016 Geneva I 26-29 September

SWIFT at Sibos

COMPLIANCE REVIEW 2016











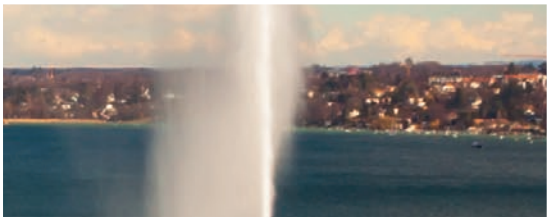

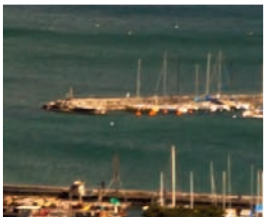





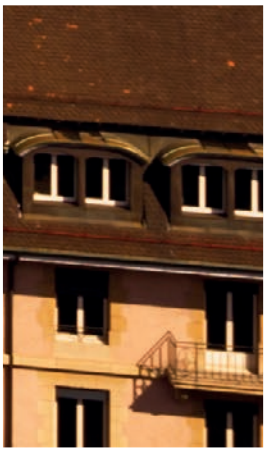

Countdown to compliance
page 3

Searching for the synthesisers
page 5

Re-assessing the risks
page 7

Joined-up thinking on fighting financial crime
page 9

Utilities build momentum
page 11

Deep thinking on the future of compliance
page 12

Know Your Challenges!
page 13

Time is of the essence
page 14

Stronger together
page 15

Scaling up on compliance
page 18

Starting out with compliance
page 19

Early stage collaboration
page 20

Maintaining compliance
page 21

Name screening
page 22

De-risking in the Caribbean
page 23

A joined up approach to compliance
page 24

SWIFT at Sibos compliance signings gallery
page 25-27

Payments Data Quality
page 26

2016

Sibos Issues

The official daily newspaper of Sibos 2016 Geneva I 26-29 September

sibos

COMPLIANCE REVIEW

COMPLIANCE AT SIBOS

Reflecting its ever-growing importance for the Sibos community, financial crime compliance was one of the four key streams at Sibos 2016. Throughout the week, the subject was discussed and debated in a variety of forums. Highlights from these discussions are included in the following pages, as reported in our two official onsite publications, Sibos Issues and SWIFT at Sibos.

Sibos Issues covers the event as a whole, while SWIFT at Sibos focuses on the latest SWIFT news at Sibos, including customer signings. We hope you enjoy this dedicated coverage of a topic that promises to remain high on the industry agenda in the year ahead.

COMPLIANCE / SECURITIES

Countdown to compliance

We are working on the due-diligence questionnaires that will enable people to assess the degree to which their counterparties are in compliance.

Mark Gem, head of compliance, Clearstream, and chair, FCCP Working Group, ISSA

#Market Infrastructures

Help is at hand for securities firms implementing ISSA's Financial Crime Compliance Principles.

The practical implications of financial crime compliance have become more tangible in the securities industry since the International Securities Services Association (ISSA) proposed a three-year time frame (to end-2018) for adoption of its Financial Crime Compliance Principles (FCCP). The adoption process requires that even long-established contractual relationships be revisited, and that their underlying documentation be redrafted into FCCP compliance. Such redrafting has to be, and has to be seen to be, a comprehensive application of due diligence.

Compliance commitment

The good news is, first, that upwards of 90% (source: ISSA) of the industry favours FCCP adoption, and secondly, that ISSA itself is committed to supporting firms through the process. Mark Gem, head of compliance, Clearstream, and chair of ISSA's FCCP Working Group, says: "We are tasked with developing tools to help our industry get to the goal of adoption. For example, we are working on the due-diligence questionnaires that will enable people to assess the degree to which their counterparties are in compliance and developing the contractual elements that firms will need." ISSA

continued on page 4

Countdown to compliance

continued from page 3

is also, says Gem, "making sure that people are aware of the tools that are available to help them cross the finishing line; things like the industry utilities; things like off-the-shelf cloud-based name-streaming solutions".

Integral to ISSA's approach is the ambition that FCCP adoption should become a virtuous cycle, progressively achieving the global propagation of best practice. This seems realistic: if the whole industry wants and is working towards compliance, it will become very difficult for a non-compliant firm to find a non-compliant counterparty. FCCP adoption seems already to be facilitating – indeed, encouraging – co-operation between firms. Thomas Zeeb, chief executive officer, SIX Securities Services, and incoming chairman of ISSA, says: "Our experience with financial crime compliance so far has been that it brings us closer to our clients. We find ourselves working together with our clients to ensure that any potentially questionable transactions are not entered into. Our collaborative approach has been received very positively, very welcomed."

Perhaps the obvious question, given the securities industry's apparently enthusiastic acceptance of both the principles and the co-operative approach to their adoption, is: how much of a burden will practical adoption impose? Discussing the three-year timeframe, James Freis, chief compliance officer, Deutsche Börse Group, says: "Going from the principles to the implementation is really quite fundamental, especially for some of the bigger institutions. We know some of the steps, but actually to amend your contracts; to have your systems ready to request and evaluate more data and keep a record of that; that will take a lot of lead time."

A matter of intent

Amending multiple contracts and systems is not a task to be taken lightly by securities services firms. But – to pose the question somewhat provocatively – couldn't we all just save time by agreeing to behave differently, and start from there? Answer: not if the ISSA principles are to be effective to their fullest possible extent. Today's regulatory environment is complex, sanctions seem to evolve and multiply, and even the simplest mistakes can be expensive. Zeeb says: "On the board of ISSA, we asked ourselves, how can we best manage the regulatory process going forward? How can we as an industry meet the intent of the regulatory requirements before a whole new series of legislation is created?" The key word is 'intent'. To comply with the letter of the law, as distinct from its intent, is to risk repeated regulatory interventions to address unforeseen 'small-print' infractions. Further, a clear understanding of the direction of travel among policymakers and regulators is most likely to result in meaningful change of behaviour rather than just check-box compliance.

> **Our experience with financial crime compliance so far has been that it brings us closer to our clients.**
>
> **Thomas Zeeb,** chief executive officer, SIX Securities Services, and chairman, ISSA

> **To amend your contracts; to have your systems ready to request and evaluate more data; that will take a lot of lead time.**
>
> **James Freis,** chief compliance officer, Deutsche Börse Group

In drafting the principles, ISSA's intent is that they should at least draw a favourable response from regulators – and the signs are that this is happening. Olivier Goffard, head of group compliance and ethics, Euroclear Group, says: "We have already had good discussions with the International Organisation of Securities Commissions and the Financial Action Task Force. We hope that in the coming months, they might recognise the principles. Having other organisations behind the principles in addition to the many ISSA member firms will make them truly robust." Regulatory approval, like the principle-based approach itself, can be 'portable' across borders. If regulators discuss and validate a set of principles, then they and the industry are saved considerable time and effort defining and implementing distinct regulatory requirements.

> **Having other organisations behind the principles will make them truly robust.**
>
> **Olivier Goffard,** head of group compliance and ethics, Euroclear Group

The fragmented regulatory environment across jurisdictions informed ISSA's approach from the outset, as most securities services firms operate across borders, and thus face a multiplicity of regulatory requirements. "We want these to be global principles," says Freis. If the objective is global acceptance, then all that time spent going back and re-establishing contractual relationships is a necessary commitment: it's the process of putting in firm foundations. Zeeb says: "There is a lot to be done, but these are things that each organisation can do on its own timeline." Given their widespread acceptance, it's easy to forget that these are voluntary principles, and that there is no actual obligation to comply with the three-year timeline. But as Zeeb notes: "Compliance isn't just about facilitating relationships with regulators; it's about protecting the enterprise and industry from criminal activity."

No short cuts

While pursuing long-term, structural changes, inevitably short-term compliance considerations also arise. There is, Zeeb suggests, a "superficially appealing" response to pressure from regulators for full mutual disclosure between parties to a transaction. It is to put in place "fully segregated accounts right the way through", in place of selective segregation and omnibus accounts. This would entail "huge change" and "huge cost" over "probably ten years". And it wouldn't be effective. Zeeb says: "We don't believe that such an approach addresses the core issue in disclosure. The fact that you know an account belongs to x, y or z doesn't help. You just end up with a huge database – you've got the haystack and you're looking for the needle. What you need is the appropriate filters to identify transactions, activities and scenarios that are questionable. You need a clear and agreed procedure for digging into those."

A clear and agreed procedure between any two parties requires mutual understanding and mutual trust – over and above any mutual obligation to hand over data. It requires, one might say, an approach based on a shared set of principles. Zeeb says: "I would much prefer transparency to be created thus: we have a questionable transaction, and we all commit to ensuring that – within the bounds of our various jurisdictional regulations – we meet the requirements of disclosure. That's collaboration focused on the exceptions and not just on the easy part of the process, which is building up the massive database." ■

Searching for the synthesisers

#Technology #Innotribe #Data

What role can third-party solutions such as 'RegTech' and industry utilities play in helping banks tackle regulatory compliance reporting challenges?

"We are drowning in information, while starving for wisdom," observed the esteemed American entomologist and biologist Edward Osborne Wilson. He predicted a future in which the world would be run by 'synthesisers', defined as "people able to put together the right information at the right time, think critically about it, and make important choices wisely".

Today's 'RegTech' innovators have staked a claim to be considered 'synthesisers' as they develop tools that aggregate and standardise often unstructured data sets to help financial institutions meet their increasingly complex regulatory compliance and reporting obligations. Moreover, their claims are being taken increasingly seriously by a wide range of governments.

In his 2015 budget, UK chancellor George Osborne called on the Financial Conduct Authority (FCA) to work with the Prudential Regulation Authority (PRA) to "identify ways to support the adoption of new technologies to facilitate the delivery of regulatory requirements". The Monetary Authority of Singapore (MAS) has appointed a chief FinTech officer to head its FinTech & Innovation Group, while Ireland has placed "research, innovation and entrepreneurship in the international financial services sector" at the heart of the government's 'Strategy and vision for international financial services 2020'. Minister of state for finance Simon Harris has placed particular emphasis on governance, risk management and compliance applications of financial technology.

In November 2015, the UK's FCA published a 'Call for input: Supporting the development and adoption of RegTech', in tacit recognition of the need for new technologies to meet financial institutions' regulatory reporting and compliance requirements. "The RegTech CFI seeks to understand technology innovation across the FinTech sector which may aid firms with their regulatory and compliance requirements," the FCA told Sibos Issues. "By launching the CFI, we question whether there is anything we can do to support the development of this sector, which stands to benefit regulated firms."

Terms of reference

From a regulatory standpoint, the terms of reference have changed, according to Brian Fahey, CEO of MyComplianceOffice (MCO), a provider of governance, risk and compliance IT solutions, with regulators focused less on assessing how a financial firm is gearing up to respond to regulation and more on the capabilities of individual firms. "The expectation is one of 'don't show me policies and procedures, but show me your reports'," says Fahey.

"The expectation is one of 'don't show me policies and procedures, but show me your reports'.

Brian Fahey, CEO, MyComplianceOffice

The use of technology to address regulatory requirements is not new. Long before RegTech came on the scene, major banks were deploying proprietary solutions, with more commoditised kit being offered to mid-tier firms by third-party technology vendors. The uptick in new regulation impacting the finance sector has caused a step change over the past decade, with firms gradually realising that 'flying solo' was costly, time-intensive and unsustainable. The result was a surge of collaboration and an increase in utility solutions to tackle specific non-competitive challenges. In some respects, these utilities have a claim to be Wilson's synthesisers too, in terms of their use of common data management processes to put together "the right information at the right time" to ensure regulatory compliance.

According to Luc Meurant, head of the financial crime compliance services division at SWIFT, utilities need four characteristics to ensure industry adoption. First, they must offer superior technologies and processes to unlock savings and increase efficiency; second, they must develop and encourage convergence in market practice and standards; third, they must deliver excellent operational management of the processes for which they take operational responsibility; fourth, they must offer a 'smart path' that enables step-by-step migration to use of the new utility, providing benefits to users at different stages.

"In the long term, common market practices must be adopted by users for utilities to work effectively, but banks can work gradually toward that goal. In the first instance, they achieve great benefits from a deeper understanding of how their peers handle the same regulatory requirements. But they don't need to move processes or transactions to a utility in a 'big bang'; perhaps identifying instead a subset of their overall business for a pilot migration, such as correspondent transactions," says Meurant.

Nor do utilities need to be all things to all people. In the financial crime compliance space where SWIFT offers The KYC Registry – a shared platform for managing and exchanging know your customer (KYC) data – Meurant predicts the emergence of separate utilities for sanctions, KYC and monitoring processes.

continued on page 6

"Regulation is forcing stakeholders to go where no financial firm has gone before.

Paul Fawsitt, CEO, MoneyMate

Searching for the synthesisers

continued from page 5

'Intelligent' data mining

Although RegTech lacks a precise definition at present, a number of common themes and characteristics suggest a long-term role on the regulatory landscape too. For the FCA, potential applications include: accelerator initiatives that focus on delivering regulatory compliance reporting; real-time risk evaluation in areas such as trade surveillance, financial crime risk monitoring, KYC and anti-money laundering (AML) requirements; data streamlining and online visualisation tools; software integration tools that interact with regulatory reporting system; and leveraging cloud-based technologies for speed and efficiency.

By seeking to unravel cluttered and intertwined data sets for the purpose of regulatory compliance reporting, RegTech aims to bring agility, speed and ease of integration to a once time-consuming and manual-intensive process. Smart analytics are then overlaid on this to 'intelligently' mine data to unlock its value and meet specific reporting requirements. Deloitte's 2015 report, 'RegTech is the new FinTech: How agile regulatory technology is helping firms better understand and manage their risks', explains how new analytics tools can use the same data for multiple purposes.

But observers suggest these efforts are still in their infancy. When it comes to mining the right data sets to comply with the raft of regulation facing financial institutions the response to date has been lagging, according to Paul Fawsitt, CEO of Dublin-based MoneyMate, a provider of data and technology solutions to the funds and banking industry. "Regulation is forcing stakeholders to go where no financial firm has gone before."

A fundamental issue is that compliance and operations professionals are having to contend with a mass of unstructured data sets from which to craft reports. "The problem is a lack of standards," says Fahey. "The more we can get to a common baseline, the better the industry will be."

The challenge is to standardise regulatory reporting around structured ontologies, which define and compartmentalise the variables for a specific set of computations, as well as establishing their inter-relationships. Fahey's MCO is a member of the Financial Services Governance, Risk and Compliance Technology Centre (GRCTC) based in Cork, Ireland, where academic and business-led R&D is being undertaken on regulatory compliance requirements facing the finance industry. Other member firms include Citi, State Street and SAP. Current research is focused on the development of 'meaning centered' semantic technologies, which rely upon an encoding process whereby 'meaning' is stored separately from data and content. At one level, it is a form of artificial intelligence which allows a computer programme to differentiate between entities. But in future this type of technology could bring order to the unstructured data sets from which financial institutions need to derive standardised and meaningful compliance reports.

Work is centred on developing families of interlinked regulatory and GRC ontologies which capture regulatory concepts, taxonomies, and rules in formal semantics. The aim is to enable efficient access to, and smarter consumption of, financial regulations and to use semantic technologies to enable smarter analysis of both structured and unstructured data. From a broader perspective, the GRCTC hopes to help the industry address a range of requirements, from pinpointing the compliance imperatives within a regulation, to measuring risk or evaluating controls.

Secure exchange

Alongside academic research and government-driven initiatives, the past 18 months has seen a rush to market of innovative start-ups, as well as new product roll-outs from established data depository and data distribution businesses. The FCA accepts the contribution of for-profit undertakings, albeit advising caution, in view of the high stakes. "Ultimately, industry must take the lead but we recognise that the FCA has a key part to play in ensuring we encourage appropriate innovation [in RegTech] that also provides proper levels of protection for consumers."

Silverfinch, a utility solution developed by Dublin-based MoneyMate, was singled out by Deloitte as an example of the type of 'disruptive' technology that will shape the future of regulatory compliance reporting. "[Silverfinch] demonstrates the power of technology disruption by turning data flow and reporting responsibility in the asset management and insurance industries on its head." MoneyMate's Fawsitt sees it slightly differently: "It's not disruptive technology, it's cohesive technology."

Launched in 2014, Silverfinch, a secure fund data utility that connects asset managers and insurers, was developed in response to the 'look-through' provision of Solvency II, which requires insurance companies to mine information on asset holdings for regulatory compliance reporting. Asset managers in turn are obliged to share information on insurers' asset holdings which, when it comes to collective investment products, can be of a highly sensitive, business-critical nature.

Silverfinch offers a single purpose-built standard utility that allows information to be exchanged in a secure, standardised format under the control of asset managers. It provides anonymity that not only protects the USP of individual asset managers but serves the compliance requirements of Solvency II. "It has the potential to revolutionise the way portfolio data is shared and disseminated among competing asset management firms," observes Fawsitt, who also sees an opportunity arising from MIFID II's transparency requirements.

> **Common market practices must be adopted by users for utilities to work effectively, but banks can work gradually toward that goal.**
>
> **Luc Meurant,** head of financial crime compliance services division, SWIFT

SWIFT's Meurant says the potential for economies of scale makes a compelling case for utility solutions in the regulatory compliance space, pointing to widely predicted rises in regulatory costs, and the continued constraints on banks' access to capital. But he acknowledges the practical difficulties faced by banks in such a fluid, fast-changing regulatory environment. "You have to be something of a visionary to adopt new approaches with a multi-year implementation timeframe at the same time as addressing day-to-day compliance requirements. With such strong, active scrutiny from multiple regulators, it's hard to step back and see the big picture," he says. Moreover, with the ultimate liability for compliance remaining with the banks themselves, any form of outsourcing must deliver standards of performance superior to the processes they aim to replace, Meurant adds.

On the RegTech front, can private initiatives alone wrestle regulatory 'big data' to the ground and come up with the secure and standardised formats that today's regulatory compliance reporting demands? For Fawsitt there is no one-size-fits-all answer. "If the industry wants more control it will either leverage what's there or reinvent it." Common sense dictates that existing 'best-of-breed' solutions will be utilised and collaborative efforts will be encouraged where progress is needed. For the FCA the answer is simple: "To meet our objectives we must coordinate with other bodies, including industry bodies." ■

> **Industry must take the lead but we recognise that the FCA has a key part to play in ensuring we encourage appropriate innovation.**
>
> **UK Financial Conduct Authority**

Re-assessing the risks

Data # Blockchain # Technology # Financial Inclusion

Serving low-risk clients in high-risk markets is made harder by financial crime compliance obligations, but not impossible.

Financial crime compliance is very different from the political processes that give rise to the rules and sanctions lists with which banks and others must comply. It is as unequivocal as a light switch: there is no gradual withdrawal of darkness, nor partial application of light. "Compliance is not negotiable," says Jochen Metzger, head of department, payments and settlement systems, Deutsche Bundesbank.

In the context of geo-political shifts, financial crime regulatory requirements are continually reshaped by events, but the obligation on banks to comply is constant, fixed and immovable.

Political leaders express goodwill towards former ideological adversaries; diplomats negotiate partnerships with once-hostile counterparties. But where sanctions apply, they remain switched on until they are switched off. "In high-risk jurisdictions, a high quality of compliance standards and their application are the crucial factor in the decision process whether business in the end will be conducted or not," says Metzger.

For international banks, de-risking options are very much on the agenda, including the ultimate don't-go-there option, which might be understandable from any individual bank's perspective, but is politically unacceptable if pursued collectively. Increasingly, the question is: can technology help banks to comply with regulations while also profitably serving low-risk customers in potentially volatile, high-risk markets? And if technology holds the key, what role does risk management play, from an overall governance perspective and on the ground?

New models, new technologies

In compliance and in banking more generally, technology is only an enabler, albeit a critical one. Compliance is not just a matter of implementing technology, however many systems, solutions and frequent upgrades it might require to keep within the rules. At the same time, changing business and risk models and emerging payments methods open up new opportunities, rendering existing remote markets more accessible. Advances in technology help make these new business models possible: more transparent transaction chains – enabled by technology innovations such as blockchain – can enable banks to nurture client relationships they might previously have shied away from.

But the compliance obligation – at the risk of repetition – doesn't change. "Independent of underlying trends in business models, legal requirements need to be applied properly. Compliance processes and their proper application must not be left behind due to innovations and possible disruptive trends," Metzger adds.

The evolution of financial crime compliance practice by banks can be viewed positively. "Compliance adds real value. It protects reputations and saves lives. If your anti-money laundering/counter-terrorism financing efforts catch something, think about what you might have prevented," says Stuart Weinstein, professor at the Faculty of Business and Law, Coventry University, and author of the International Securities Services Association's study on 'Transparency in Securities Transactions and Custody Chains'. Weinstein argues that financial crime compliance is a "societal responsibility" for individual banks and the wider banking industry alike – a responsibility that is shared by regulators even more than it is overseen by them. This suggests we all have a role in maintaining compliance. But Weinstein goes further: "International banks and the whole banking system are an essential infrastructure. Banks can't cut out whole sections of the globe from the international market. They have to find better solutions than that."

Opportunity cost

An analogy: if you're getting burnt, withdraw your fingers from the stove. It is wholly rational – and compliant – to address "extremely big penalty risk" by withdrawing from relationships, and indeed, from whole markets – Somalia, for example. Cutting out whole sections of the globe, as Weinstein puts it, is an extreme form of de-risking, and in the short term, it does indeed amputate a whole set of risks. But to sever an array of relationships, to withdraw from a geography, is not only to cut off today's dialogue; it is to put the phone down on tomorrow's potential, which may be harmful to future profits, more so to political stability. "As banks de-risk, people invest less in their due-diligence processes and they invest less in their correspondent-banking relationships, and it really should be the other way round," says Weinstein.

For banks unwilling to accept the opportunity costs inherent in extreme de-risking Weinstein highlights possible ways forward. "International banks and their correspondents have to work together. Blockchain technol-

continued on page 8

continued from page 7

ogy has the potential to introduce transparency throughout the transaction; payment-screening processes and the use of greater information helps as well. Data analytics is very promising," he says – concluding with the suggestion that a "good-faith standard" backed by technology-enabled transparency and mutual understanding may be more effective than today's strict-liability standard.

Consulting Group McKinsey & Company put out a paper in January 2016 – 'A best-practice model for bank compliance' – that gives an interesting slant on de-risking. The paper's authors, Piotr Kaminski and Kate Robu, director in McKinsey's New York office and principal in the Chicago office respectively, argue for "active ownership of the risk-and-control framework" alongside "integration with the overall risk-management governance, regulatory affairs, and issue-management process". The paper makes a very neat point: "Compliance risks are driven by the same underlying factors that drive other banking risks, but their stakes are higher in the case of adverse outcomes … Therefore, it's only fitting that a modern compliance framework needs to be fully integrated with the bank's operational-risk view of the world."

In the current environment, compliance considerations are inherent in the business of banking. But if improvements in technology and processes allow banks to engage with risk rather than stepping away – even where that might seem the prudent move – how do we exploit the opportunities while avoiding the pitfalls? Beyond core compliance, what are the next steps to safely banking low-risk clients in high-risk jurisdictions?

It should be possible for correspondent banks to safely bank low-risk clients in high-risk jurisdictions. However, the underlying risks involved need to be addressed and minimised.

Jochen Metzger, head of department, payments and settlement systems, Deutsche Bundesbank

Risk and reward

For reasons of politics and profits, banks must be able to support sound business cases when the appropriate opportunity arises. "In principle, it should be possible for correspondent banks to safely bank low-risk clients in high-risk jurisdictions. However, the underlying risks involved need to be addressed and minimised by applying compliance standards and requirements accurately. Compliance and its proper application may not only add value to an evolving correspondent model, but in the end may be the key to conducting business successfully at all," says Metzger.

Compliance requires engagement, and engagement requires communication, and ultimately, the determinant of successful compliance is the communication of best practice down to the local level. As well as enterprise-wide risk management policies and processes that are coordinated and calibrated to the bank's overall risk appetite, this 'risk-sensitive' approach to financial crime compliance also demands education, if not enterprise-wide then certainly at several levels within the bank, especially for client-facing staff. While bank staff need constant education in understanding and identifying the different types of risk that new clients and markets represent, they too can be the educators. As a compliance culture evolves and takes root within banks, and the understanding of compliance obligations become embedded, there is also an opportunity to educate local clients on how to comply with sanctions and identify behaviours and patterns consistent with criminal activity.

We have the technology and the will. We can, as Weinstein suggests, save lives. So, is it time to take the more extreme de-risking options off the agenda of effective compliance? Do we have the skills and the tools to achieve the levels of engagement needed to safely bank low-risk clients in high-risk jurisdictions? Given the penalties for non-compliance, it's a judgement every bank must weigh seriously and continuously. "The solution to that one," Weinstein says, "is the customer-relationship person at the local bank. Every day, people who work in those banks have to deal with these situations; every day, they have to rely on their gut sense, which is usually right. They're the unsung heroes of compliance." ■

Banks can't cut out whole sections of the globe from the international market. They have to find better solutions than that.

Stuart Weinstein, professor at the Faculty of Business and Law, Coventry University

Joined-up thinking on fighting financial crime

Stuart Levey was appointed to the newly-created position of chief legal officer of HSBC Holdings in January 2012. Prior to joining HSBC, he had served in both the US Department of the Treasury and the US Department of Justice, which he joined from private practice in 2001. While at the US Treasury between 2004 and 2011, he served as first under secretary for terrorism and financial intelligence under Presidents Bush and Obama.

#Payments #Financial Inclusion

Opening Sibos 2016's compliance stream, Stuart Levey, chief legal officer of HSBC Holdings, made the case that now is the time to build 'true' collaboration between government and the private sector to combat financial crime and preserve the integrity of the global financial system. A combination of factors – notably a broad acceptance of the effectiveness of financial tools in fighting financial crime and concerns about financial exclusion due to de-risking – provide an opportunity for increased momentum on information-sharing issues, argues Levey.

Sibos Issues: What do you consider the single biggest risk and compliance challenge facing the banking industry today?

Stuart Levey: In addressing this issue, the biggest challenge the industry faces right now is how to achieve a greater level of 'true' collaboration between government and the private sector in the fight against financial crime. It is an area in which the private and public sector have a shared goal of preserving the integrity of the financial system and detecting and preventing financial crime. While there has been some progress, up until now they have been pursuing this largely by relying upon completely different sets of information and not collaborating as well as they could. There is of course required reporting and there are also some good pilot efforts to enhance information exchange. But we are still a long way off of a dynamic, real-time conversation between government and the financial sector in which there is a regular flow of information.

I have witnessed this from both sides, having served in government and in my present role at a global financial institution, and conclude that we are not reaching our true potential. The absence of this kind of dynamic dialogue – and the barriers that exist to sharing information cross-border within an institution, among institutions, and between government and the private sector – means that we are lagging behind criminals and others who seek to abuse the financial system who are operating in a cross-border, high-tech fashion.

The challenge is not new and the audience attending Sibos are familiar with the need for greater information-sharing and collaboration. But there are two factors that make this moment in time the best opportunity we have ever had, at least since I started working on this in 2001, to achieve real progress.

One, there is definitive evidence that the fight against financial crime is here to stay. It has become a critical component of governmental policy. In the past, the value of fighting financial crime was not always clear, but this is no longer the case. The power of efforts in this regard over the last 10 years has been demonstrated. As just one example, the Iran nuclear deal showed how effective the use of financial measures can be. Before efforts to pressure Iran financially started in 2006, many people had been sceptical that financial measures, and in this case especially sanctions, could have any real impact. Now it's clear they created leverage that laid the groundwork for a deal; the only debate is whether the leverage was used wisely. There has also been success in tackling terrorism financing, as demonstrated by the diminishing effect it has had on the core of al-Qaeda. Today, the whole world stands convinced by the power of financial measures. Once a new set of policy agenda items for governments, it is now embedded as a viable policy tool.

The second factor stems from the phenomenon of de-risking. Banks, out of a desire to keep financial crime out of their institutions, have increasingly implemented de-risking initiatives, ex-

continued on page 10

continued from page 9

iting high-risk categories of clients and curtailing operations in high-risk jurisdictions. This has had the unintended consequence of exacerbating the problem of financial exclusion. In our effort to prevent financial crime we need to ensure innocent people are not excluded from the financial system.

To accomplish both objectives calls for a highly targeted and precise approach to tackling financial crime. And to achieve this outcome requires increased collaboration and information-sharing both between government and the private sector and amongst the financial sector itself.

Sibos Issues: How do you overcome vested interests and divergent governmental priorities to create a 'true' spirit of collaboration at both a pan-industry level and between governments?

Stuart Levey: Attention is now front and centre on de-risking and avoiding the unintended consequence of financial exclusion. These are real policy problems for governments. Government agencies are warning against a blanket approach to de-risking. This now forms a part of the G20 agenda. The highest level of government is grappling with the problem of financial exclusion and the lack of availability of correspondent banking services in certain countries. At the same time, there is a strong desire to be even more effective in fighting financial crime. The solution to both of those issues is better collaboration and the improved analysis of information that will stem from that. Then both government and industry will be able to better focus their efforts on the truly bad actors.

Sibos Issues: How high a priority is this for banks?

Stuart Levey: My impression is that this is a very high priority across the industry and will stay that way for the foreseeable future for a number of reasons. In part this stems from success at a policy level in pursuing initiatives to counter illicit finance and preserve the integrity of the financial system, which will remain a top priority. There is also a shared interest among government and the private sector to tackle financial crime more efficiently and effectively, something that can only be achieved through close collaboration and better sharing of information.

Sibos Issues: Tackling financial crime is a board-level priority. As such, should banks be focused on the composition of the board, appointing non-executive directors with expertise in counter-terrorism and combatting criminal activity?

Stuart Levey: It is clearly useful to do that and is the approach HSBC has taken. Lord Evans* sits on our board, having previously served as the director-general of MI5. Jim Comey** also served on the HSBC board prior to his appointment as the director of the US Federal Bureau of Investigation in 2013. A board-level committee has also been established which includes former government officials and advises the bank on issues relating to financial crime. By bringing this type of expertise in-house we are actively creating connectivity to the issues in the fight against illicit activity. It creates a dialogue at another level about how to do this better.

In the UK, this approach has gone some way to yielding an initiative called 'JMLIT', the Joint Money Laundering Intelligence Taskforce, a collaboration between the UK government on the one hand and a number of banks, including HSBC, on the other. Up to 20 international banks are involved, along with the British Bankers' association. They are working collaboratively with the UK's financial crime agency to share information and analysis to better determine the true scale of money laundering and the methods used by criminals and terrorists to exploit the UK financial system. This is step one on a long road. I am encouraged though. One of the footnotes to the political change in the UK is that this type of collaborative initiative was promoted and supported directly by Theresa May when she was home secretary. That should be seen as a positive in terms of the political will and support we expect to receive as we move forward.

> **In our effort to prevent financial crime we need to ensure innocent people are not excluded from the financial system.**
>
> **Stuart Levey,** chief legal officer, HSBC Holdings

Sibos Issues: Is this level of active governmental support mirrored elsewhere and how do you go about incentivising public and private partnerships of this kind?

Stuart Levey: There is progress toward similar initiatives in the US. The industry has to tell governments: 'Look, you want to do two things. You want to fight financial crime effectively, while ensuring this doesn't simultaneously lead to financial exclusion as a consequence of de-risking. We agree with you on both objectives and the way to achieve a positive outcome is to collaborate and gain better access to data and thereby fight financial crime more effectively. It will be an iterative process, in the sense that we will be providing you with information and you can tell us whether it is helpful or not and that will help us in turn give you better information.'

In this way, we will be able to better target bad actors in the financial system without compromising access to banking services for innocent clients. Real-time collaboration is the way to get this done. It is not the way we have done things in the past. The whole suspicious activity report filing system is important, but it is neither real time nor is it iterative. We can do it better.

This is the type of dialogue that boards and senior executives can engage in with government. These are the things we as an industry should be actively supporting, because in the end we all stand to benefit.

Sibos Issues: What is the cost of failure if, despite the best intentions, government and the industry fail to truly collaborate in the fight against financial crime?

Stuart Levey: One of two things will happen. Either we will not be effective in keeping illicit actors out of the financial system or we will be ineffective at avoiding financial exclusion as a consequence of not being precise enough in our efforts. That's what failure means to the industry. What failure means to an institution we are all quite familiar with and that is what drives the incentive to de-risk.

Sibos Issues: What you outline amounts to a 'call to action'. What do you want to see come out of Sibos in terms of 'next steps' in moving the debate forward?

Stuart Levey: I would like to see a political commitment and imperative to pursue collaboration, even to the extent of looking at the legal barriers that exist now to that collaboration.

> **There is a shared interest among government and the private sector to tackle financial crime more efficiently and effectively.**
>
> **Stuart Levey,** chief legal officer, HSBC Holdings

We need a true dialogue with the industry about what the legal barriers are and how they could be removed. I'd also like the industry to make clear that our desire for collaboration is well intentioned. Our intentions here are to truly protect the integrity of the financial system. It is great to be more efficient and cost-effective but the real incentive here is to protect the financial system. If people understood there were good intentions on both sides I think we could make the necessary reforms as well as forging greater public and private collaboration. I'd also like to see recognition that JMLIT is the kind of initiative we could do more robustly to change the whole environment.

Sibos Issues: Beyond Sibos, is there a role for SWIFT in promoting this agenda?

Stuart Levey: The answer to that is yes. There are already tools that SWIFT offers that are very effective. From where SWIFT sits in terms of its unparalleled access to information it has the potential to be a key player in the kind of effort I am talking about. If we were able to effectively address the privacy and confidentiality issues and derive the benefit of the data that SWIFT collects, it could potentially play a quite dramatic role in fighting financial crime.

Sibos Issues: How do you address the delicate balance between preserving the confidentiality of SWIFT data and utilising its content to fight financial crime?

Stuart Levey: The role I performed in a previous life makes me highly sensitive to the complications that exist. In my experience, when people focus seriously on sharing information for a particular, valid purpose on the one hand and on the other are serious about protecting privacy a way can be found. While a challenge, I don't consider this an insurmountable obstacle. ■

***Jim Comey served on the Board of Directors of HSBC Holdings until July 2013.*

Utilities build momentum

#Data

As banks increase adoption, will financial crime compliance utilities take on an even wider remit?

The benefits of using industry utilities to manage financial crime compliance and know-your-customer (KYC) data have become more widely accepted in recent years. As such, banks are being urged to be more ambitious in their participation in such utilities to maximise potential efficiencies while supporting compliance effectiveness.

"We need to be more innovative with utilities, but one of the challenges we face is the fear factor that is often linked to innovation. We need regulators, banks and intelligence services to work together with the same objective of better managing financial crime risk," says Barbara Patow, global head of anti-money laundering at HSBC.

Sharing resources

The financial services industry has already made significant progress in sharing resources to meet financial crime compliance objectives, a key milestone being the launch of The KYC Registry in December 2014. Operated by SWIFT, the facility enables participating banks to avoid duplication of effort by sharing KYC data in a controlled environment, thereby mitigating risk and reducing costs. The facility announced its 2,000th customer in January and has recently surpassed 2,700 member institutions.

A number of utilities are now addressing a range of different compliance tasks and challenges. Their arrival has been welcomed as a step forward in efficiency by removing some of the 'hygiene factors' around data collection. However, some banks are still dealing with internal challenges that prevent them from sharing data with other entities.

"Most banks have recognised the value of sharing resources rather than having to do their own KYC due diligence on every individual counterparty, but it is taking time for utilities to gain traction, both with the banks and their underlying clients," says Matthew Russell, partner in the financial crime team at PwC.

Following the strategic decision to use a utility, banks will need to adjust to the operational implications in order to realise the full range of benefits. But once a bank has invested, the start-up time required to collect and contribute its own data, it can soon achieve efficiency benefits by consuming data from other institutions through The KYC Registry. The bank can then look to take advantage of the enhanced effectiveness resulting from the higher quality information and free up staff time to focus on analysis rather than data collection.

Before this, however, banks' operations and compliance teams need to commit and successfully engage with a utility. Relying on a third party to help deliver on a bank's regulatory responsibilities can require a big shift in culture, Russell explains.

"Operations staff have often been at the forefront of exploring the potential cost savings associated with utilities, but they haven't always taken compliance with them on that journey. In many cases, compliance staff will take some convincing and that's a process that may still need to be worked through," he says.

Encouraging adoption

Utility operators acknowledge that it will take time for banks to fully embrace utilities and are keen to engage with the industry to increase usage. Despite The KYC Registry's strong take-up rate, SWIFT remains focused on encouraging further adoption, and on adding new services. For example, users can now access Dow Jones 'negative news' content which makes up part of the risk-based approach to customer due diligence.

"We need to focus on making sure institutions feel comfortable adopting utility solutions. Typically there are many different players involved in a bank's client onboarding and KYC processes, so inevitably it takes time to connect the different workstreams and ensure the central ownership that is critical to integrating a KYC utility service into a bank's existing processes and operations," says Bart Claeys, head of KYC compliance services at SWIFT.

Moreover, banks' internal compliance programmes have typically developed over many years and these established processes cannot be changed overnight. Claeys says, "We are very confident, however, that utilities will ultimately deliver major cost and efficiency benefits and support greater transparency, particularly in regions where regulation is less stringent, compliance programmes are less advanced, and where de-risking is a concern."

And, while some institutions might still need to bring all of the necessary internal stakeholders on board to enable them to benefit from utilities, others are already looking to expand their scope beyond basic KYC and due diligence functions to derive benefits in other areas. HSBC's Patow believes there is a desperate need for greater industry cooperation on transaction monitoring and screening, even though sharing transaction-level data may be more complex than client-level data.

"The way transaction monitoring has been done in the past is ineffective because we have to filter through a large volume of noise to identify the relevant data. It is still early days, but we are looking at how we can leverage the successes in KYC and be more creative in transaction monitoring," says Patow.

Central to the discussions around transaction monitoring will be finding a way for utilities to respect and uphold the confidentiality of data and satisfying data privacy laws while also meeting regulatory and banks' own requirements. In the age of big data and highly sophisticated cloud-based technology, such challenges shouldn't be insurmountable, but it may take time before substantial progress is made.

"Both KYC and transaction monitoring are non-competitive areas for banks, so there is widespread agreement on the benefit of sharing intelligence. We need to work together so that we can realise the benefits and demonstrate the potential opportunities across financial crime compliance," Patow explains.

Future directions

Using a trusted third party to assist in the process of transaction monitoring may offer the opportunity not just to cut costs, but also to improve quality and effectiveness of banks' financial crime prevention and regulatory compliance efforts. Whereas an individual institution only ever has a partial view of a particular transaction, an independent utility has a broader view and may be better placed to detect and report suspicious activity.

"The use of utilities is gradually beginning to move beyond due diligence to other aspects of financial crime compliance and it does make sense to look at sharing transaction data so that a third party can get a better view of what activity might warrant investigation by authorities," says PwC's Russell.

For the utility operators themselves, there are clearly questions to be answered about the direction they will take in the future, not just in terms of the additional services they will offer, but also the extent to which they will choose to focus on specific functions or geographies as financial crime compliance requirements evolve.

To date, The KYC Registry has maintained a specific focus on correspondent banks and funds players, although SWIFT is engaging with other industry groups and utility providers to look at other areas of cooperation. While most utilities have focused on a particular niche up until now, some believe there is a case to be made for greater collaboration.

"There are multiple KYC utilities in co-existence, and this could remain the case over the longer term if each utility addresses different market segments. However, the benefits to the industry in terms of lower cost and greater efficiency could be amplified by increased interoperability and linkages between the different utilities. That should be one of our goals for the future," says Claeys. ■

We need to be more innovative with utilities.

Barbara Patow, global head of anti-money laundering, HSBC

The use of utilities is gradually beginning to move beyond due diligence to other aspects of financial crime compliance.

Matthew Russell, partner, financial crime team, PwC

Deep thinking on the future of compliance

#Data #Payments #Technology

Advances in machine-learning techniques are extracting more content and context than ever before, even from unstructured data. How can such innovations help to create more cost-effective compliance monitoring solutions?

> **Everyone realises that machine learning is the future.**
>
> **Anthony Fenwick,** global head of AML compliance, treasury and trade solutions, Citi

It's hard to put a figure on the 'true' cost of compliance to the banking industry. It's easy, however, to conclude the cost is big, very big, and growing. In 2015, a Financial Times article estimated that the annual outlay for some banks was upward of US$4 billion. For individual institutions, sums twice this amount have been suggested. There is no doubting the fact that banks' compliance headcounts have risen sharply into the tens-of-thousands. The cost of recruiting chief compliance officers is often cited as one of the reasons executive pay continues to climb. But as banks are being pressed by regulators to improve their compliance monitoring and reporting capabilities, other forces are compelling them to rein in costs across the board.

"Everyone realises that machine learning is the future," says Anthony Fenwick, global head of AML compliance, treasury and trade solutions at Citi. Not only is the cost of compliance running into the hundreds-of-millions, he observes, but the focus of banks' investment on compliance needs to shift. Over the last decade, much of the investment has been around rules-based scenarios to monitor and root out suspicious activity. "This is simply not cost-effective," says Fenwick. The process involved in filing a suspicious activity report is lengthy, labour-intensive and more often than not fruitless. Detection and execution ratios are poor.

A big part of the problem is that banks are bogged down by running multiple legacy systems. For the purpose of monitoring transactions, data from all these systems has to feed in together. "This can cause havoc with monitoring," explains Fenwick, "especially because the more you try and get out of it, the more data-hungry it becomes." One of the biggest problems with a monitoring system is that when an alert is generated, it becomes necessary for the appropriate data sets to be identified and unravelled, taking account of different systems and, in the case of the largest banks, contending with regional variances.

"Compliance is a huge cost of doing business today," acknowledges Dan Adamson, founder & CEO of OutsideIQ, a compliance-focused cognitive solutions developer. Much of that cost is human, with banks creating armies of people to monitor transactions and investigate alerts. Adamson sees this as a 'knee-jerk' reaction by banks, throwing bodies at the problem when the regulatory bar is raised. While this approach has allowed banks to continue to conduct business, it is far from optimal and comes with a significant price-tag. A lot of compliance work is done in duplicate, even triplicate, because it is so error prone. There is a huge overhead to recording everything and making it auditable. "It is not only inefficient, it is ineffective: a lot of money laundering isn't caught," says Adamson. "We have created this monster that spits out millions of alerts," concurs Fenwick.

How to be smart

There is common consensus that banks need to find a more intelligent solution. Prior to founding OutsideIQ six years ago, Adamson joined Microsoft to work on Bing, the web search engine owned and operated by the software giant, where he focused on refining its vertical search strategy. OutsideIQ was established on the premise that the machine-learning techniques and vertical search algorithms used for consumer site searches could be adapted for business to help deal with risk. "We have incubated a technology that is now a cognitive computing platform based on machine-learning techniques and focused on identifying risks," explains Adamson.

While the underlying platform is ubiquitous, OutsideIQ has developed products that serve specific use cases, including a due diligence product, DDIQ, geared to identifying risks around on-boarding clients. By relying on machine-learning techniques it allows users to conduct due diligence in a highly reproducible, auditable and cost-efficient manner, explains Adamson. Work that was previously undertaken manually can be done by computers. "It clears the noise," he explains, enabling banks to move up to 95% of their KYC workload into a machine-operated AI environment.

Citi's Fenwick supports the development of machine-learning based products that are built for a specific use case. Today, the compliance process is hampered by banks relying on a single 'catch-all' monitoring system that runs similar risk scenarios, irrespective of client type or the market in which they operate. "At present it is a catch-all that catches little and that is the problem," says Fenwick. The monitoring process as it stands fails to distinguish in a meaningful way between a hedge fund and a large corporate client, for example. "These are very separate and distinct businesses and we are going to have to start creating different monitoring platforms," says Fenwick.

One example of a specific use case might be correspondent banking, where Fenwick sees a potential role for SWIFT in developing a tool to monitor transactions using machine-learning techniques, supported by human oversight and guidance. Ideally, he would like to see a tool developed that allowed the bank to eliminate MT 202s from its roster of items to monitor, a move which he says could potentially save millions of dollars.

Human dimension

While there is agreement on the benefit of machine-learning techniques, there is no room to become over-evangelical about their application. One of the historical failings of monitoring systems is that they have been left solely to technologists and operational teams to build. "This results in a monitoring system operating like a mathematical model, rather than an investigatory tool designed to detect someone who is undertaking criminal activity," says Fenwick.

"One of the pitfalls with machine learning is to think that monitoring is something you can leave solely to a computer," he adds. Although AI functionality can make a significant contribution to compliance monitoring by eradicating the mundane and stemming unnecessary errors, the human element is still critical. Machine-learning solutions will ultimately allow banks' compliance teams to move away from an approach that monitors every transaction coming down a pipe, to concentrate instead on the pathways that throw up abnormalities.

This is an approach that Adamson supports. While a great advocate of machine-learning techniques in the here and now, he believes computers have a defined place, albeit a very important one, in the compliance process. Machines can be very good at weeding out 95% of the noise, but a human 'last step' will be necessary for a final review leading to action. In the very near future, Adamson predicts, we will see more people working on the smarter oversight aspects of compliance, with the routine groundwork having been laid by machines. ■

Know Your Challenges!

#Innotribe #Technology

KYC due diligence continues to require high levels of manual processing for banks. Can collaborative innovation deliver new efficiencies? SIbos Issues spoke to panel participants ahead of the Sibos session on the Innotribe Industry Challenge on Compliance.

Thursday at Innotribe is going to be "very interesting", says day anchor Leda Glyptis, director at financial markets consulting group Sapient. "I participated in the Industry Challenge on Compliance in London in July, and I'm very excited by the discussions we'll have today about it. The winning solution was a really interesting product – it was visually impactful, it was innovative, and it solves a problem we have today," Glyptis continues.

The first session of today's programme will include a detailed account of the motivation and process behind Innotribe's Industry Challenge on Compliance, before revealing the successful participants and explaining next steps. To help delegates gain a deeper understanding of the potential benefits of technology innovations in the compliance space, the session's core themes will include: the need for a collaborative approach to compliance challenges; the crucial role of technology – and innovation – in securing banks and their clients against fraud and money-laundering in particular; and the need for standardisation across know-your-customer (KYC) and anti-money laundering (AML) due diligence processes, and compliance function in general.

Joining Glyptis on stage for the 'Innotribe Day Opening and Industry Challenge on Compliance' session will be Anju Patwardhan, Fulbright visiting scholar at Stanford University and former chief innovation officer at Standard Chartered Bank, as well as Kevin Johnson, head of Innotribe innovation programmes at SWIFT.

Identifying need

The overall objective of Innotribe's Industry Challenge programme, launched this year, is to bring a collaborative approach to developing practical solutions for business areas with outstanding needs to be addressed. To find and meet the most pressing needs, the Innotribe team works closely with SWIFT customers to identify the specific business areas that could benefit most from collaborative solutions. From this follows an exploration of potential opportunities in specific business areas, typically leading to the development of proofs of concept and thence, ideally, to new and tangible solutions for the industry.

In the compliance space, The KYC Registry, a SWIFT utility that supports the financial crime compliance efforts of correspondent banks, had already demonstrated the value of collaboration. However, both SWIFT and Innotribe wanted to explore the potential benefits further, in response to growing industry need.

> **The aim of the Industry Challenge is to foster innovation through collaboration, and thereby reduce the cost of compliance.**
>
> **Bart Claeys,** head of KYC compliance services, SWIFT

> **Banks need to find ways to become more capital and cost-efficient.**
>
> **Anju Patwardhan,** Fulbright visiting scholar, Stanford University

According to Patwardhan, the regulatory climate has done much to shape banks' need for more cost-effective compliance solutions. Fast-evolving KYC and AML rules have placed financial crime compliance high on the agenda of senior managers across the banking sector, while new restraints on capital, leverage and liquidity are forcing banks to manage and contain, where possible, the rising costs associated with compliance.

"Due to regulatory changes in parameters for credit risk-weights, for many of the same risk profiles as before, banks need more capital today. They also need more liquidity. Essentially, they need to find ways to become more capital and cost-efficient," says Patwardhan.

Effective compliance is thus key to the future, and the effective deployment of innovative new technologies and new ideas is becoming ever more crucial.

Effective and efficient

For Innotribe's Industry Challenge on Compliance, the first step was the initial collaborative work on articulating the challenge itself. "We decided to concentrate on new compliance products around the KYC marketplace," says Johnson. The focus was on developing new CDD (customer due-diligence) and EDD (enhanced due-diligence) products to complement The KYC Registry. "Until now, CDD and EDD processes, within the overall KYC function, have typically required significant manual effort, and thus cost," says Bart Claeys, head of KYC compliance services, SWIFT. "The aim of the Industry Challenge on Compliance was to foster innovation through collaboration, and thereby to reduce both the cost of compliance and the time-to-implementation of new efficiencies. This was in response to the urgent need, expressed by the correspondent banking industry in particular, for utility solutions that increase effectiveness and efficiency, eliminate manual processes, and provide global standards and processes where possible.

Having established the product focus for the July event, Innotribe team members identified relevant vendors. Once that point was reached, Innotribe brought SWIFT customers and internal teams together with solution providers and FinTech start-ups. In effect, a multi-disciplinary team was assembled that could address a challenge from all angles within a workshop environment - the third stage in the Industry Challenge process. "This was developed specifically because banks and customers have expressed the view that they are no longer satisfied with traditional procurement processes that stifle rapid innovation and delay deployment of new products and systems," says Johnson.

Typically, the workshop stage telescopes much of that process into a period of (very intense) days, demonstrating the value of collaborating around a clearly articulated goal. "The workshop replaces the lengthy and costly process of scheduling and conducting numerous pitch meetings," says Johnson. The Industry Challenge on Compliance took the form of two distinct workshops. The first, for established firms, was a one-day 'marketplace challenge' for vendors wanting to build products that would form part of a marketplace linked to The KYC Registry. The second challenge, for start-ups, ran over two days and was broader in scope, with five start-up vendors pitching to work on new products in the KYC and compliance space in general.

After the workshop comes the nitty-gritty of collaborative development. "We selected two vendors from the marketplace challenge to work with us on developing new solutions linked to The KYC Registry, and two start-ups to develop proofs of concept around new ideas in the compliance space," says Johnson. ■

Time is of the essence

While fraud detection and AML monitoring display synergies, these compliance disciplines take place over different time horizons, posing barriers to a joined-up approach.

Time itself is the key challenge in joining up the two disciplines of fraud detection and AML monitoring. On the one hand, fraud detection operates in a real-time environment to prevent monetary loss for customers and banks alike; on the other, AML monitoring is undertaken primarily to meet a regulatory requirement and as such exists in a world of batch cycles. While fraud detection tends to be more preventive, AML is more investigative.

Arriving at a joined-up approach "is about leveraging synergies, while respecting the differences", said Cate Kemp, group payments compliance director at Lloyds Banking Group.

Common ground?

At Credit Suisse, fraud and AML are treated organisationally as a unified problem, focusing on the policy framework and trying to leverage a common understanding across the disciplines to achieve a more simplified structure from a control standpoint. "The underlying infrastructure, technology and data, and the viewpoints that you are trying to get to, are common. We are trying to leverage these similarities," explained Ben Hargreaves, director, global head of anti-fraud, Credit Suisse.

In the context of client accounts, a lot of the data points used to assess different types of financial crime activity are common to both fraud detection and AML monitoring in terms of understanding beneficial ownership, the origins of a transaction and the beneficiaries that are involved.

"The differences are around the timings of interventions," explained Hargreaves. From an AML perspective, real-time processes are not as critical. To prevent fraud occurring however, the timeliness of the decision-making process plays a significant part.

At a policy, level firms need to have a risk appetite that transcends any type of financial crime, said Kemp. It is in the timeliness of the intervention where both the challenge and the opportunity lie.

While the data is the same and the processes involved are inherently similar, whether onboarding or conducting KYC checks, most banks remain siloed in their approach to compliance, with different parts of the organisation undertaking separate checks, said Angus Wildblood, partner for enterprise risk services at Deloitte. The objectives in the different parts of the organisation also diverge. From a fraud perspective, the aim has been to manage risk and save money, said Wildblood, while AML is more focused on managing a regulatory position. One key step toward achieving a more joined-up approach would be for banks to move away from viewing AML as a compliance-driven discipline towards a financial crime risk-management undertaking, said Wildblood.

However, Jeremy Warren, head of CIB global financial crimes compliance, JP Morgan, said fraud and AML *are* connected in the area of investigations case management. Ideally, disclosures should be made through the same system, allowing staff to look at compliance issues from different angles, while retaining a holistic view across a client relationship. This is a prerequisite for taking informed decisions, said Warren.

> **Cross-functional training is an important element.**
>
> **Ben Hargreaves,** director, global head of anti-fraud, Credit Suisse

Client dimension

Looking at fraud prevention and AML monitoring from a customer perspective, improvements will come from banks offering a 'one touch' approach, rather than maintaining separate lines of enquiry, said Hargreaves. "If we manage fraud and AML together, we then have a better chance of preventing clients from becoming victims of crime," said Wildblood. From the perspective of becoming a customer of a bank there is only one process involved in onboarding, he added, to ease the burden on the client.

"Bringing fraud and AML together passes the logic test," said Kemp. But theory and reality currently diverge. Proactively contacting clients to protect them from becoming victims of crime can result in unpredictable consequences, she noted. A practice designed to prevent harm can result in customers complaining about intervention, with banks accused of interfering or stalling legitimate payments.

It follows that client education is a prerequisite to achieve a joined-up approach, said Warren. "There is a lot of synergy between fraud and AML, but client outreach and communication covering both is vital."

Cultural shift

Regulators expect banks to achieve financial crime compliance, whether sanctions screening, protecting against fraud or AML. For banks, the question of how to arrange their compliance skills to achieve efficiency and effectiveness is key. This requires an ability to leverage knowledge and experience across different compliance teams, panellists agreed. "Cross-functional training is an important element of this," said Hargreaves, in order to enable staff with broader experience to detect financial crime from a holistic viewpoint, rather than simply through the prism of AML, fraud or sanctions screening respectively. The danger that comes with too narrow a focus on one or other discipline is that illicit activity is missed because it fails to fit a specific set of criteria. "Sharing lessons learned in different parts of the organisation is critical," said Warren.

> **Bringing fraud and AML together passes the logic test.**
>
> **Cate Kemp,** group payments compliance director, Lloyds Banking Group

This leads to conversations at an enterprise level around transaction monitoring. The feedback loop is considerably faster in preventing a fraud than AML. "It's not the same in the AML world," acknowledged Hargreaves. Through education and sharing knowledge, the aim is that some of the embedded practices that fraud detection has brought over time, such as using advanced analytics-modelling capabilities and rapidly adapting to client behaviour changes, can be introduced to AML for the benefit of all. ■

Stronger together

Collaboration and information-sharing between institutions and across the public and private sectors will be vital in fighting financial crime and preserving the integrity of the global financial system.

There is a need for wholesale reform in the way financial crime is tackled. This was the blunt message delivered by Stuart Levey, chief legal officer, HSBC, and keynote speaker at the opening of Sibos 2016's compliance stream.

"We are poised to create the momentum to make a true paradigm shift," said Levey. Two countervailing forces are at play; a deep public policy commitment to combat financial crime and preserve the integrity of the financial system, coupled with growing concern among policy-makers over the unintended consequences of financial exclusion through de-risking. "De-risking is being applied as an alternative to managing risk," cautioned Levey.

To reconcile these imperatives, more precision is required in how illicit conduct within the global financial system is targeted. This can only be achieved by improving collaboration and information-sharing across the public and private sector, said Levey. There are four critical components to this increased level of interaction. It has to be cross-border, in real time, among private sector actors, and between government and industry.

"The case for a new standard on information sharing is overwhelming," said Levey. The Financial Action Task Force (FATF) has a critical role to play. "They could set standards around the sharing of information for financial crime risk management."

Information-sharing takes many forms – between regulators and banks, within and between banks, between banks and their clients, and between banks and third parties such as utilities, to name a few. Over the course of four days, panels and presentations across Sibos 2016's compliance stream explored all these and more in detail, with the aim of enhancing industry efficiency and effectiveness in tackling financial crime.

> **The case for a new standard on information sharing is overwhelming.**
>
> **Stuart Levey,** chief legal officer, HSBC

Zero tolerance

De-risking was the focus of Monday's panel, 'How to safely bank low-risk clients in high-risk jurisdictions'. Banks were de-risking correspondent relationships even before FATF mutual evaluations were done, said Julie T Katzman, chief operating officer at the Inter-American Development Bank. "Banks looked like they were developing a zero tolerance on the risk spectrum."

Correspondent banking relationships decreased significantly over the course of 2014 and 2015, noted Richard Lalonde, senior financial sector expert, IMF. The effect was most marked in the Caribbean where more than a dozen indigenous banks have had their relationships severed with global banks. "There's a danger that some countries could be cut off the global payment network," said Jochen Metzger, director general of payments and settlement systems, Deutsche Bundesbank.

What seemingly amounts to a blanket approach to de-risking is due in part to banks operating in an environment in which they are unsure what regulators will do. "That cre-

continued on page 16

ATTITUDES TO UTILITY SOLUTIONS

Current use of shared utilities for compliance

71% implementing
18% evaluating

Areas of compliance suitable for utilities

80% KYC
64% sanctions screening
62% AML

Source: Digital polling during 'Utilities: Reaching the tipping point?' session (27 Sept 2016)

continued from page 15

> **The decline and concentration of correspondent banking is a cause for concern for regulators globally.**
>
> **Alexander Karrer,** chair of the correspondent banking coordination group, Financial Stability Board

ates fear and when banks make decisions based on fear, they do not tend to optimise," said Katzman.

Correspondent evolution

The need for clarity from regulators was echoed in the session, 'Evolution of correspondent banking', which examined the impact of increased financial crime compliance obligations on the correspondent banking model. "Regulators need to give us clear standards," said Patricia Giangrande, global head of business control office, institutional cash management, Deutsche Bank.

"The decline and concentration of correspondent banking is a cause for concern for regulators globally," observed Alexander Karrer, Switzerland's deputy state secretary for international finance, speaking in his capacity as chair of the correspondent banking coordination group at the Financial Stability Board (FSB). This can affect the ability to send and receive international payments and drive financial flows underground, he cautioned.

Faced with sanctions compliance, a nuanced approach to de-risking is called for. Larisa Zalomikhina, group head of compliance at Sberbank, said it was imperative that customers understood and identified different types of sanctions. In the case of Russia, she said, "It took time to explain that restrictions applied to long-term financing and not correspondent banking."

The cost and inconvenience caused to customers by correspondent banks' financial compliance measures could play a significant role in their ultimate effectiveness, suggested Olivier Denecker, director of knowledge, McKinsey. To this end, regulators should focus as much on the cost of compliance as its effectiveness. "It is where you draw the line on risk," he said.

Karrer agreed there was a need to distinguish between higher and lower risk situations in correspondent banking and that this was an area being explored by the FSB. "There is no intention to add additional layers of regulation. Rather, we are looking to provide clarity and to make regulation as effective and cost-friendly as possible," he said.

continued on page 17

> **Regulators need to give us clear standards.**
>
> **Patricia Giangrande,** global head of business control office, institutional cash management, Deutsche Bank

continued from page 16

FIGHTING TERRORISM

Banks are fighting terrorist financing effectively in the view of two-thirds of the audience canvassed at the session on 'Recent trends in counter terrorist financing'. The panel begged to differ. "The large-scale attacks in Paris and Brussels were a wake-up call," said James Freis, chief compliance officer, Deutsche Börse." There is a funding element to all these attacks. There are many sources of intelligence but the financial component is critical because it represents one of the concrete steps in uncovering a terrorist network."

Recent developments are challenging banks to update their approach to tackling terrorist financing, according to Tom Keatinge, director of the Centre for Financial Crime & Security Studies, part of the Royal United Services Institute, a London-based think-tank. This was not a criticism, he said, merely a reflection of the switch by terrorists from the formal banking system to use less 'auditable' channels.

Closer collaboration is needed between financial institutions and intelligence services, said Troels Oerting, group chief information security officer at Barclays and former director of operations in the Danish Security Intelligence Service. While panellists agreed that public and private partnership was key, Keatinge stressed the importance of gaining access to higher value information, while Oerting acknowledged the challenges in balancing security and privacy. Put to a vote, two-thirds of the audience felt that banks' should agree to sharing confidential information within an appropriate framework. It reflected a change of mindset, noted Freis.

> **The whole concept of a utility is about breaking down barriers.**
>
> **Barbara Patow,** global head of money laundering, financial crime compliance, HSBC

Tipping point

Are shared utilities reaching a tipping point? That was the central theme of the panel focusing on compliance utilities. For David Fleet, managing director, client onboarding & management at Standard Chartered, the answer was a qualified "yes" when it came to The KYC Registry and its use in correspondent banking for onboarding and review. At a regional and national level, utility solutions are gaining momentum for a variety of purposes, such as SIRESS for cross-border payments between member countries of the Southern African Development Community. "It remains to be seen what will happen on a global scale, but certainly within local and industry-specific areas we are definitely reaching a tipping point," concluded Fleet.

"Reaching a tipping point doesn't mean we are out of the woods in terms of how we will best use utilities," observed Mark Gem, chief compliance officer and member of the executive board, Clearstream. While bank-to-bank KYC is forging ahead, in the world of the end-client and corporates, the jury is still out, he said.

On the subject of further mutualising financial crime compliance costs and efforts, Matthew Russell, partner, financial crime, PwC, said there was a lack of consensus between banks over use of internal versus third-party sanctions screening solutions. "The whole concept of a utility is about breaking down barriers," said Barbara Patow, global head of money laundering, financial crime compliance, HSBC. "As banks we have to get together, dispel the fear factor and innovate."

Mother of invention

Banks have always been able to make a virtue out of a necessity. Opportunities to extract value from compliance data were discussed in the session, 'Utilising compliance data assets to generate new business opportunities'. Jim Wadsworth, managing director, Accura at Vocalink, said the UK payments processor was already aggregating billions of transactions annually to create a real-time picture of the UK economy. "That is potentially valuable from a public policy or capital markets perspective."

Although almost a quarter of audience members said they were already reusing data collected for compliance purposes to personalise banking products and services, with a further 20% at a planning stage, over a third had no plans. The panel felt the polling provided an accurate reflection of the market, with Eric Clapton, head of retail financial crime prevention programme, Lloyds Banking Group, encouraging banks to utilise their investment in compliance to create sustainable resources. ■

Scaling up on compliance

Financial crime compliance has risen steadily up the agenda of global industry regulators since 2008. SWIFT is keeping pace accordingly.

"Financial institutions not only need to implement the right controls for sanctions screening and other compliance initiatives, but increasingly need to demonstrate that those controls are running effectively," says Luc Meurant, head of SWIFT's compliance services division. "This is becoming increasingly challenging for banks with competing claims on available resources. Banks are looking for new ways of meeting the required level of effectiveness in their compliance processes in line with their risk appetite and while managing costs with cost pool."

For Meurant, this trend is fostering the emergence of compliance utilities for the industry. "Interestingly," he notes, "we are sensing an increased openness toward utilities from regulators and even encouragement for initiatives that are well framed and operated."

As a result, SWIFT is rapidly expanding its compliance services suite. "We started in an area very close to our business – Sanctions Screening – then added other services like The KYC Registry," says Meurant. "Our board and community have asked us to further step up our game and we have received a clear mandate from our community to develop compliance capabilities for the SWIFT ecosystem. Compliance is one of the three pillars of SWIFT's 2020 strategy, and we have a bold roadmap in place to build three interconnected and complementary compliance utilities over the next five years in the areas of Sanctions, Know Your Customer (KYC) and Analytics / Anti-Money Laundering (AML)."

> **"We aim to cover the full scope of requirements and make the various components of our offering interoperable.**
> Luc Meurant, SWIFT

At Sibos 2016, compliance was one of the four conference streams running throughout the week. The stream will provided delegates with insights into the broader context of financial crime compliance, while also providing information on the latest tools, tactics and strategies available to SWIFT community members.

Auditorium sessions

The SWIFT Auditorium sessions meanwhile outlined what SWIFT's compliance offerings can do for the business today and what new solutions the cooperative is developing to help institutions manage their sanctions, KYC and AML compliance activities. Over the course of the week, SWIFT showcased a range of compliance-related products and services. These covered the entire transaction lifecycle, from using The KYC Registry and SWIFT's new Name Screening service to decide whether or not to accept a particular business relationship, to screening financial transactions on an ongoing basis with Sanctions Screening and tracking traffic patterns and correspondent risk using Compliance Analytics.

What is crucial, says Meurant, is to ensure that every utility – from sanctions to KYC and analytics / AML – targets distinc-

continued on page 19

continued from page 18

tive needs and segments. "That way, as a community, we really benefit from economies of scale."

One impact of this more comprehensive offering should be a reduction in the cost of due diligence processes. The tools will also be useful for institutions that think they could be vulnerable to de-risking – the termination of correspondent relationships because of (perceived) compliance cost and risk. "The best thing that potentially vulnerable banks can do is demonstrate that they have implemented the expected compliance controls so their counterparties can accurately assess the potential risk of onboarding them as clients," says Meurant. "Due diligence costs can be as much as $50,000 per year for high-risk counterparties, so smaller banks should take any steps possible – such as joining The KYC Registry and using Sanctions Screening to screen transactions – to protect themselves by reducing compliance cost and risk for their counterparties."

SWIFT continues to evolve across the entire compliance portfolio, says Meurant. "Banks' needs continue to change as regulation evolves. We aim to comprehensively address our community's needs and make the various components of our offering interoperable. All of these solutions are driven by the community." □

Starting out with compliance

Financial crime compliance is critical to every SWIFT user. SWIFT is evolving its compliance portfolio to meet both changing regulations and the need for interoperable processes along the customer relationship life-cycle.

Expanding its compliance services suite is one of three pillars in SWIFT's 2020 strategy. As regulations change, so do the requirements of SWIFT's customers.

"We continue to see a move beyond mere 'box-ticking' to embedding compliance firmly in institutions' business practices and cultures," says Brigitte De Wilde, head of financial crime intelligence and services at SWIFT. "SWIFT's vision is to provide a cohesive suite of services that address the compliance requirements of financial institutions throughout the customer lifecycle."

For ease of presentation, De Wilde divides the life cycle into two stages: customer onboarding; and the ongoing customer relationship. A range of compliance processes must take place during both stages in line with the bank's risk appetite and regulatory obligations.

Prior to onboarding a new correspondent, a bank will typically identify and perform initial risk assessments on a number of prospects. At this stage, Bankers World Online, part of the SWIFTRef portfolio, offers a useful starting point for client identification information. Bankers World Online focuses primarily on payments processing data, SSI information, as well as risk and credit ratings. "Typically, clients worldwide use Bankers World Online to prospect for potential commercial counterparts that fit the risk profile they want," says Bart Claeys, head of KYC compliance services at SWIFT.

Once a potential counterpart has been selected, performing client identification and Know Your Customer (KYC) activities is essential to ensure that the counterpart does indeed meet the risk parameters set by the bank and that individuals associated with it. Here banks can count on The KYC Registry, SWIFT's centralised repository of standardised due diligence information about correspondent banks, funds distributors and custodians.

The KYC Registry provides an efficient, shared platform for storing, managing and exchanging standardised KYC data. SWIFT has worked with the world's largest correspondent banks to define a set of data and documents that addresses KYC requirements across multiple jurisdictions. Bankers World Online has been integrated with The KYC Registry to provide easy access to an even broader, more granular set of KYC information.

"Industry adoption of The KYC Registry has been tremendous," says Claeys. "The Registry is being used by more than 2,800 correspondent banking and funds institutions to reduce the cost and complexity of KYC activities, and increase the effectiveness of their KYC programmes."

For banks in higher-risk markets, the Registry presents a golden opportunity to demonstrate transparency and compliance and safeguard their connections to banking services and the global economy. In an environment where 'de-risking' is increasingly seen by many large transaction banks as a necessary process to meet their own compliance goals, the Registry provides a line of defence for smaller banks, enabling them to demonstrate transparency and that they have their own robust checks in place.

Another important onboarding step is screening customer names. SWIFT is launching a new Name Screening service to screen individual names as well as client, supplier and employee databases. Such screening helps banks avoid business relationships with individuals and entities on international watch lists, and enables them to implement the proper due diligence for higher-risk customers.

> **"Clients worldwide use Bankers World Online to prospect for potential commercial counterparts that fit the risk profile they want.**
>
> Bart Claeys, SWIFT

"As a hosted service, Name Screening will provide a powerful screening solution that's as simple to use as a search engine, along with the ability to automate database screening as part of business as usual AML processes," says Nicolas Stuckens, head of sanctions compliance services at SWIFT. "Name Screening, together with Sanctions Screening, Sanctions Testing and new list management services, will form a cohesive Sanctions Utility that delivers tools our customers need in order to better manage sanctions compliance across their organisations and throughout customer relationships."

continued on page 20

continued from page 19


Nicolas Stuckens, SWIFT

A final step in onboarding is the setup of SWIFT's Relationship Management Application (RMA) and RMA Plus. These SWIFT-mandated authorisations let users specify which types of messages they are willing to exchange with specific counterparts, and blocks any traffic not meeting those criteria. As such RMA is increasingly seen as a compliance control. Indeed, some regulators require banks to do full due diligence on their correspondents whenever an RMA is present, regardless of whether a business relationship is actually in place. □

Certifying compliance effectiveness

Banks operating in New York State will soon be required to comply with new regulations which require them to test, ensure and certify that their transaction monitoring and filtering programmes are operating effectively. The new regulation has four main components. Banks need to:

- Maintain an appropriate transaction monitoring programme
- Maintain a watch list filtering programme
- Perform tests and ongoing analysis to ensure that systems are working correctly
- Submit an annual board resolution or senior officer compliance finding stating that the bank's transaction monitoring and filtering programmes comply with the regulation.

While the regulation specifically applies to financial institutions operating in New York State, it has implications for banks headquartered in other markets. The new rules, which take effect on 1 January 2017, could also indicate the direction which other regulators may take in the future.

Sanctions testing

Banks can use SWIFT's Sanctions Testing product to test, fine tune and understand their sanctions filters and list data. Unlike tests which focus only on a subset of data, Sanctions Testing takes a comprehensive approach to assurance and coverage testing by incorporating every dimension of the relevant messages. This gives greater confidence that all necessary data has been looked at.

Sanctions Testing enables banks to improve filter efficiency by identifying ways to reduce false positives, and establishes a baseline from which to measure the impact of subsequent tuning iterations on the institution's risk appetite.

Detailed reporting demonstrates the impact of changes to filter settings and enables banks to document filter performance to management and overseers. As such, Sanctions Testing gives banks the confidence needed to certify compliance with Section 504.3 of the new DFS regulation.

Early stage collaboration

SWIFT has long encouraged collaboration to address common problems. With the Industry Challenge programme, Innotribe is taking this philosophy one stage further.

Monday's opening session at Innotribe provided an opportunity to introduce the Industry Challenges – a new Innotribe initiative designed to identify and validate innovative, utility-based solutions to the most pressing challenges faced by SWIFT's member organisations.

The Industry Challenge is modelled around five phases: Define; Discover; Zero-to-Test; Collaborative Development; and Go-to-Market.

The objective of the first phase is to identify a common problem that needs to be tackled. The Discovery phase involves the identification of key stakeholders who should be included in the challenge: SWIFT Business and IT representatives; member institutions; external providers; partner institutions; and carefully selected startups.

This year, after consulting with SWIFT community members, Innotribe confirmed the themes of the first two challenges: Distributed Ledger Technology (DLT) for securities, as well as Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) for compliance solutions.

Securities

The Industry Challenge for Securities challenges participants to build the lifecycle of a short-dated bond on Blockchain. In April, a group of experts and vendors met in London to commence the Zero-to-Test workshop. For two days the group engaged in demos, use-case discussions, proposal development and pitching. Three startups were selected to progress their Proofs of Concept in the next 12-week phase with support from SWIFT and participating member banks.

Feedback from the Industry Challenge for Securities was overwhelmingly positive. "The creation of SWIFT was one of the greatest examples of collaboration among competitors ever accomplished in the financial industry," said one global bank innovation lead. "What I've seen over the last few hours is the most impressive example of collaboration among competitors I've seen within SWIFT since its inception."

Compliance

In July, the SWIFT Compliance team and Innotribe worked closely together to help shape the challenge, select the startups and bring customers and representatives from major banks to participate in a collaborative workshop in London.

At the end of the two days, as with the Securities challenge, two startups were chosen by attendees to further develop their concept for a three-month period, in collaboration with Innotribe and SWIFT,

continued on page 21

continued from page 20

with funding, coaching and direct contact with SWIFT member institutions.

Introducing the event, Kevin Johnson, head of Innotribe innovation programmes at SWIFT, set the scene, stressing how participants were chosen "not for their impressive products but for their technology."

Johnson adds, "We want to explore how we can use this technology to the advantage of our customers, as we believe that technology can help develop new solutions and products, and we can do this not only *for* our customers but *with* our customers."

"The initial Industry Challenges have gone well and we going to do more," says Johnson. "As financial technologies evolve, Innotribe will continue to play a vital role in bringing the startup ecosystem and financial services expertise together. This is not about us going out and finding solutions to recommend. This is about the customer saying, 'here's my problem' – to which we can respond 'here are the potential FinTechs who can help'."

In consultation with SWIFT's customers and member institutions, the Innotribe team is creating a portfolio of different challenges for the years ahead, drawing on SWIFT's global network to bring together the most relevant participants for each event. □

"Innotribe will continue to play a vital role in bringing the startup ecosystem and financial services expertise together.

Kevin Johnson, SWIFT

Participants gather for Innotribe's Industry Challenge for Securities

Maintaining compliance

SWIFT provides an expanding portfolio of services to help banks comply with regulation around correspondent relationships.

For banks, financial crime compliance involves far more than simply reporting periodically to the appropriate bank supervisor. It requires a number of controls by correspondent banks; from correspondent onboarding through to the flow of daily business, as well as periodic reviews of each relationship.

As explained in the Tuesday edition of SWIFT at Sibos, SWIFT's KYC Registry, Bankers World Online and the new Name Screening service support customer due diligence and screening requirements during customer onboarding.

Once counterparties have entered into a commercial relationship, different requirements come into play. Here, SWIFT provides services to screen transactions, track ongoing behaviour and monitor risk in customer relationships.

Community utilities

"SWIFT's vision is to provide utility solutions that meet our customers' compliance needs throughout the customer lifecycle," says Nicolas Stuckens, head of sanctions compliance services at SWIFT.

These requirements include screening transactions between counterparties, testing that screening systems are performing properly, performing ongoing Know Your Customer (KYC) and Customer Due Diligence (CDD) activities, and maintaining a global overview of transactions and correspondent relationships in order to identify and investigate areas of potential or elevated risk. SWIFT already offers services in each of these domains.

Sanctions Screening, the first compliance service launched by SWIFT, surpassed 500 customers in August 2016. A fully hosted solution, Sanctions Screening checks financial transactions against more than 30 watch lists to ensure compliance with sanctions regulations. It simplifies sanctions compliance by providing a full solution that includes a screening filter, up-to-date sanctions lists, case management and quality assurance.

Many institutions already have complex and highly customised screening systems in place, but they may lack the assurance that these systems are working. Here SWIFT offers Sanctions Testing, which enables banks to test and tune the effectiveness and efficiency of their transaction and name screening filters and lists. Sanctions Testing also helps banks address increasingly strict regulatory requirements, such as new rules from the Department of Financial Services (DFS) in New York which will require institutions to test and certify the performance of their screening systems and programmes.

Know your customer

Knowing who you are doing business with – and understanding whether and how those relationships are evolving – is at the heart of compliance programmes.

continued on page 22

continued from page 21

More than 2,800 correspondent banking and funds institutions are using The KYC Registry to reduce the cost and effort of ongoing due diligence.

By maintaining a standardised set of each member institution's KYC data and documentation in a single, secure location, The KYC Registry is driving major efficiency gains during annual reviews – and customer onboarding.

"Once a relationship is established, KYC reviews tend to be conducted annually, depending on whether the client is considered high-risk or not," explains Bart Claeys, head of KYC compliance services, SWIFT. "If you detect unusual behaviour or a change in ownership or management, that might also trigger a review in the interim."

The frequency and level of detail required for KYC reviews does typically depend on the level of risk assigned to each correspondent relationship, and whether changes in behaviour might indicate greater risk.

Analytics

SWIFT transaction data plays an important role in evaluating behavioural changes by correspondents, and SWIFT provides advanced data analytics tools to help customers fully leverage such insights.

Compliance Analytics provides visibility on end-to-end flows between different customers, highlighting unusual or high-risk behaviour and risk concentration. Used by more than 30 of the world's largest banks, it also gives banks unique visibility on activity shares in high risk corridors, and into their Relationship Management Application (RMA) authorisations, enabling the identification of dormant or unused relationships that might pose unnecessary compliance costs, or potential risk.

"Compliance Analytics provides unique visibility on a financial counterparty's transaction activity and enhances banks' efforts to prevent illicit behaviour.

Brigitte De Wilde, SWIFT

"Compliance Analytics provides unique visibility on a financial counterparty's transaction activity and enhances banks' efforts to prevent illicit behaviour," says Brigitte De Wilde, head of financial crime intelligence and services at SWIFT. "It helps you monitor your historical data regularly to identify trends, spot anomalies and spikes, and detect potential policy breaches."

SWIFT recently expanded its Compliance Analytics suite with a new Payments Data Quality service that helps banks comply with FATF Recommendation 16 and related regulation that tightens requirements around originator and beneficiary data in payments messages. The service helps banks evaluate the quality of originator and beneficiary details in the payments they send and receive, and highlights correspondents and branches whose payments tend to lack the required data.

The next addition to the Compliance Analytics portfolio will be an AML Correspondent Monitoring module, to be launched early next year. Designed to address the specific compliance requirements of correspondent banks, the module will enrich a counterparties' risk profile by providing risk metrics for KYC reviews, and risk assessments and rich AML transaction monitoring using a more granular approach than traditional AML transaction monitoring systems. Banks will be able to use AML Correspondent Monitoring as an automated transaction monitoring tool to identify specific, unusual or high-risk patterns of activity to be reviewed as part of 'Business As Usual' (BAU) AML processes.

With so many factors in play, financial crime compliance is, to some extent, a moving target. "Across the entire portfolio we continue to evolve to meet changing requirements," says De Wilde. "We provide use cases on how best to deploy each product and tool, but each bank will apply them in different ways. What SWIFT is doing is to provide an effective technology response to a range of compliance and business requirements."

The KYC Registry's benefits will be explained during the SWIFT Auditorium session: The KYC Registry – A global experience, at 15:30 today. □

Name screening

As announced by SWIFT's chairman Yawar Shah during Monday's opening plenary, SWIFT is introducing a Name Screening service to enable banks and corporates to screen their client, supplier or employee databases for names appearing on sanctions, politically exposed persons (PEP) and private lists. The service will provide online search engine-style lookup of individual names as well as automated batch screening of entire databases, such as consumer and supplier lists.

"The addition of Name Screening is an important step in the development of our Sanctions Utility, which will also provide standardised sanctions lists and a platform for institutions to manage and automate list updates," says Nicolas Stuckens, head of sanctions compliance services at SWIFT.

Name Screening leverages SWIFT's highly successful, industry-driven utility model to deliver intuitive, easy-to-use case management, a world-class screening engine and advanced list technology. SWIFT will standardise public sanctions lists to increase accuracy and reduce false positives and will source politically exposed persons (PEP) lists from industry leader Dow Jones.

Online lookup will be available in January 2017, with the full database screening solution to follow in Q3 2017. Learn more this afternoon at 13:00 in the SWIFT Auditorium during the session Introducing Name Screening: Screening your customers and suppliers just got easier.

De-risking in the Caribbean

In the last few years, the correspondent banking industry has been increasingly impacted by the trend of de-risking; the decision taken by banks to rationalise their correspondent banking relationships.

Decisions on de-risking are typically driven by concerns about money laundering and terrorist financing, as well as by cost and regulatory pressures. While this trend has affected banks around the world, research published by the World Bank in November 2015 found that the Caribbean was the region most significantly affected. According to the report, a majority of the region's banking authorities reported a significant decline in foreign correspondent banking relationships.

Willemstad, capital of Curaçao.

Why de-risking?

According to the Centrale Bank van Curaçao en Sint Maarten (CBCS), the general view of the local banking sector is that de-risking occurs for a number of reasons. These include increasing regulatory requirements, strategic decisions to stop offering correspondent services in particular markets, and insufficient business to justify the risks and due diligence costs associated with correspondent banking relationships.

The implementation of global regulatory standards has meant that banks face increased compliance costs in providing correspondent banking relationships. "In addition, tax information-sharing agreements that also result in more costs for the correspondent banks have added to the de-risking trend," notes CBCS.

Indicating the scale of the issue, CBCS reports that 14 de-risking events have occurred in the last year in Curaçao and Sint Maarten. Other research has shown that in the Eastern Caribbean, one correspondent bank terminated all accounts involved with downstream correspondent or third-party intermediary activities, as well as closing accounts of several legal professionals and local charities.

The implications of de-risking are particularly significant given that the region's correspondent banking relationships tend to be concentrated with a small number of banks. "A 2015 Caribbean Association of Banks (CAB) survey of members indicates a heavy reliance on one or two US correspondent banks to provide key services, such as payment processing, third-party payments and cash clearing," says Mary Popo, general manager of the CAB.

Impact of de-risking

This trend has significant implications for the region's banks and their end customers. CBCS notes that correspondent banking relationships are crucial for financial institutions – especially for smaller standalone banks and international banks – given the limited access to foreign financial markets.

Where end customers are concerned, the impact of de-risking could include making it difficult for people to pay for consumables imported from the US, according to Trevor Brathwaite, deputy governor of the Eastern Caribbean Central Bank (ECCB). "In addition, a number of our citizens send their children to universities in the United States," he says. "If fees and accommodation costs cannot be paid, children will not be able to advance their education."

For banks which have been on the receiving end of a de-risking exercise, there is a clear and urgent need to put replacement correspondent banking relationships in place. Brathwaite says that some second-tier banks in the US have indicated a willingness to provide services to Caribbean banks – although these arrangements have yet to be finalised.

CBCS notes, however, that "It is not easy for the banks to establish new correspondent banking relationships. Most respondents that experience a de-risking event have not been able to establish new relationships due to the significant and time-consuming due diligence process required prior to entering into a new relationship."

Overcoming the challenges

A number of different options are under consideration to address these issues. Brathwaite says that actions being taken include diplomatic discussion at the highest political level, as well as making sure that robust legislation is in place. "We are also exploring the possibility of having our own clearing bank in the US," he says. "Some see that as far-fetched, but we are working on a proposal in conjunction with the Caribbean Development Bank."

CBCS reports that Curaçao has adopted

> **"With over 2,800 financial institutions already signed up, The KYC Registry gives banks a means of providing validated information to their correspondents in a standardised way.**

continued on page 24

continued from page 23

several pieces of AML/CFT legislation in order to comply with international standards and execute the action plan recommended by the Caribbean Financial Action Task Force (CFATF). Sint Maarten is in the process of reviewing the draft of its AML/CFT legislation with the same intention. "CBCS hopes that FATF draft guidance on correspondent banking services will increase the likelihood of US banks maintaining correspondent banking relationships. This assumes that the main reason for US banks currently ending their correspondent banking services is down to the perceived risks involved," CBCS commented.

Brathwaite adds that the ECCB is recommending that banks use The KYC Registry, SWIFT's repository for KYC information. With over 2,800 financial institutions already signed up, the Registry gives banks a means of providing validated information to their correspondents in a standardised way.

At an individual bank level, there may be other actions that banks can take to avoid being de-risked. By providing greater transparency over their activities, business lines and behaviour, banks can share information more effectively with counterparties, provide greater levels of comfort and reduce due diligence costs for their correspondents.

Finally, for correspondent banks that may be considering a de-risking exercise, alternative actions should be considered, says Popo. "We would like correspondent banks to implement measures to mitigate risk, rather than de-risking. They should also provide timely communication of compliance gaps, enabling the respondent bank to address the issues, while working with them to enhance collaboration, trust and transparency." □

A joined up approach to compliance

Over the past few years, financial crime compliance has moved centre stage at Sibos. This year, it comprised one of the four main conference themes.

At the opening of the compliance stream on the first day of Sibos, Stuart Levey, chief legal officer at HSBC and a former US under-secretary for terrorism and financial intelligence, warned that the financial industry has some way to go in matching its disparate approaches to compliance with the aims of governments and society in combatting criminal activity and terrorism. "The dots are not being connected, and certainly not in a real-time, iterative, and dynamic way," he said. "If we do not collaborate better, we risk being one step behind in our efforts to keep illicit actors out of the system while also exacerbating the problem of financial exclusion."

For Paul Taylor, head of financial crime compliance initiatives in the Americas, United Kingdom, Ireland and the Nordics, SWIFT, these observations chime with SWIFT's own engagement in helping its community meet its compliance challenges. "Particularly interesting for us was the way Stuart Levey made a strong call for rethinking the way banks and regulators address compliance, including issues of data privacy and data sharing," he says.

SWIFT's involvement in compliance reflects a consensus view in the financial services industry that compliance is not a competitive differentiator, since everyone has to do it. Over the week, notes Taylor, it became clear, through the digi-voting results in the various sessions, that many participants are either using or considering using utilities as a way of meeting compliance requirements and are looking to extend that use to related domains such as sanctions.

SWIFT itself announced two new services during the Sibos week; Name Screening and a Payments Data Quality analytics and reporting service. "We received a very positive reaction from the community in both cases," says Taylor. Introductory auditorium sessions were followed by numerous meetings and product demonstrations in the SWIFTLab.

> **"Our customers have embraced the concept of secure, cloud-based transaction screening solutions, and have asked us to extend this model to the screening of names and databases.**
> Paul Taylor, SWIFT

Payments Data Quality

Payments Data Quality is a reporting and data analytics service to help financial institutions comply with new international requirements for originator and beneficiary information in payments messages.

Recommendation 16 from the Financial Action Task Force (FATF) requires originator and beneficiary information to be included in wire transfers. However, says Taylor, "The lack of standard practices for formatting some originator and beneficiary details, such as addresses and bank account numbers, can make data detection by automated systems difficult. The Payments Data Quality service provides a review of messages using verification rules developed by SWIFT in line with industry practice."

The Sibos Auditorium session on Payments Data Quality introduced Nordea Bank as the first subscriber to the service. Lene Hedegaard Baltzarsen, senior financial anti-crime manager, Nordea, was optimistic that the service will strengthen defences for the community as a whole. "As this is a collaborative tool, banks will benefit from each other's experience," she said.

One aspect of the new services is a list of 'dummy names' – such as Mickey Mouse, or 'My customer' – that SWIFT has detected in some payments messages instead of accurate originator and beneficiary information. This list will be shared with Payments Data Quality customers to create a collaborative list of words that should trigger further investigation.

Name Screening

The first version of SWIFT's Name Screening service, due to be launched in January, was also unveiled. "Our customers have embraced the concept of secure, cloud-based transaction screening solutions, and have asked us to extend this model to the screening of names and databases," says Taylor. Name Screening combines a screening application with automatic list updates, alerts and a case management system. "Financial institutions can use the tool when onboarding new customers or

continued on page 25

continued from page 24

when carrying out one-off checks of individuals or entities, while corporates can use it to check the names of suppliers and customers," says Taylor.

The new service will screen against official sanctions and private lists as well as lists of politically exposed persons (PEPs) and their relatives and close associates (RCAs). SWIFT is partnering with Dow Jones to provide access to high-quality relevant risk and compliance data.

Introducing the service during the Auditorium session, Nicolas Stuckens, head of sanctions compliance services, SWIFT, pointed out that Name Screening complements SWIFT's existing transaction screening service, Sanctions Screening, allowing for a more streamlined approach to screening customers. "At many firms, information about customers and suppliers is dispersed across different systems and databases," he commented. "Name Screening will enable firms to automate screening through a single platform for greater accuracy and efficiency, as well as providing a demonstrable audit trail."

SWIFT's aim is to create a comprehensive screening utility service, covering transactions, names, list management and quality assurance, while helping to define common market practices, says Taylor. As of 2017, SWIFT's portfolio will also include Daily Validation Reports to allow customers to identify unexpected changes associated with payments to counterparties.

Underpinning compliance efforts is the need for transparency – which Taylor suggests could help mitigate the potential consequences of de-risking for counterparts in high-risk jurisdictions; an issue to which Levey referred in his opening address. "If you are a smaller bank in a riskier jurisdiction and you become transparent making it easier for your correspondents to collect the documentation they need to reassure their own regulators, you may have less to worry about in terms of de-risking," he says.

Beyond the new services recently launched or in the pipeline, Sibos also provided an opportunity to unveil the work that SWIFT's compliance team is doing with Innotribe through its industry challenge. "We are working through proofs of concept with selected FinTechs and expect to have further exciting news by Sibos in Toronto," says Taylor. □

SWIFT at Sibos compliance signings gallery

Banco Santander signs for Compliance Analytics

Banco Santander has signed up for Compliance Analytics, a SWIFT service that helps financial institutions mitigate financial crime risk and cost.

Left to right: Thierry Chilosi, SWIFT; Stéphanie Rodriguez Aniorte, Santander UK plc; Gema Montoya, SWIFT.

Northern Trust subscribes to SWIFT KYC Registry

SWIFT's KYC Registry was developed in collaboration with major global banks and provides a streamlined, global centralised repository and data sharing platform for KYC compliance information.

Left to right: Paul Taylor, SWIFT; Justin Chapman, Northern Trust, Global Head of Market Advocacy & Innovation Research; Felina Solomon, SWIFT.

Rabobank goes live with KYC Registry and Compliance Analytics

"With Compliance Analytics you get a better view on transactions with geographic risks, "

Ingmar Kramer, Financial & Economic Crime (Sanctions).

Left to right: Olivier Lens, SWIFT; Annick Roelants, SWIFT; Ton Versteeg, Rabobank.

Payments Data Quality

SWIFT's new Payments Data Quality service is an advanced reporting and data analytics solution that helps financial institutions comply with new international requirements for originator and beneficiary information in payments messages. The new service helps banks monitor their compliance with the Financial Action Task Force's (FATF) Recommendation 16 for wire transfers, issued in 2012.

There is widespread recognition within the global banking community that not all payments messages contain adequate and complete originator and beneficiary information.

Payments Data Quality was cited in a recent Financial Stability Board (FSB) report as an important industry action to support payments message quality.

Nordea Bank AB recently became the first subscriber to the new service, which helps banks detect whether originator and beneficiary information is missing or incomplete in the payments messages they receive or send.

"High-quality payments data is vital to a broad range of compliance activities, including sanctions screening, transaction monitoring, and the detection of data anomalies in payments messages," says Lene Baltzarsen, Senior Manager, Nordea Bank AB. "Nordea is committed to demonstrating industry leadership in sanctions risk management, and SWIFT's new Payments Data Quality service represents a major step forward in supporting our compliance with the new FATF Recommendation 16 requirements and enhancing the overall effectiveness of our financial crime compliance programme."

Nordea Bank becomes first customer of SWIFT´s new Payments Data Quality Service

The Swedish financial services provider will use SWIFT's new service to support compliance with stricter requirements for originator and beneficiary information in payments messages.

Left to right: Simon Muir, SWIFT; Lene Hedegaard Baltzarsen, Nordea; Erica Ahman, SWIFT.

Raiffeisen Bank International signs up for SWIFT's Compliance Analytics service

RBI will use reliable SWIFT data to complement its existing monitoring systems, support KYC processes, and extend correspondent risk assessment across its operations and group entities.

Left to right: Judit Baracs, SWIFT; Sven Refflinghaus, SWIFT; Tatjana Dobrovolny, Raiffeisen Bank International; Susanne Prager, Raiffeisen Bank International; Sabine Zucker, Raiffeisen Bank International; Axel Summer, Raiffeisen Bank International; Michael Formann, SWIFT.

Euro Exim Bank signs for KYC

Left to right: Guy Sheppard, SWIFT; Sanjay Thakrar, Euro Exim Bank Ltd; Graham Bright, Euro Exim Bank Ltd.

Sumitomo Mitsui Banking Corporation has signed up for SWIFT's Sanctions Testing Service

Sumitomo Mitsui Banking Corporation (SMBC) has chosen SWIFT's Sanctions Testing Service to ensure their filters' effectiveness and improve system efficiency.

Left to right: Andrew Burlison, SWIFT; Hiroshi Kawagoe, SMBC; Airo Shibuya, SMBC; Youngsoon Suh, SMBC; Luc Meurant, SWIFT; Yuji Takei, SWIFT.

Van Lanschot Bankiers signs up to SWIFT's Payment Data Quality tool

Left to right: Olivier Lens, SWIFT; Ernst Jansen, F. Van Lanschot Bankiers.

Northern Trust engages SWIFT Compliance Team for Sanctions Testing assessment

Northern Trust has engaged SWIFT Consulting Services for Sanctions Testing to supplement the programmes and people they already have in place. SWIFT's Sanctions Testing product is widely used by teams at leading institutions worldwide to test, tune and optimise their transaction, customer and PEP filters.

Left to right: Paul Taylor, SWIFT; Justin Chapman, Northern Trust, Global Head of Market Advocacy & Innovation Research; Felina Solomon, SWIFT.

Bank of Communications group subscribes to SWIFT KYC Registry

Bank of Communications, one of the five largest banks in China, has subscribed to the SWIFT KYC Registry as a group for its international footprint expansion.

Left to right: Mr. Zhang Wan Yin, Bank of Communications Co., Ltd; Daphne Huang, SWIFT.

Central Bank of Curaçao and Saint Maarten supports KYC Registry adoption in community

Left to right: Jairo Namur, SWIFT; Glensher Maduro, Centrale Bank van Curaçao en Sint Maarten; Paul Taylor, SWIFT.

ABC signs for SWIFT's KYC Registry

Left to right: Eddie Haddad, SWIFT; Jianyao Qu, The Agricultural Bank of China; Daphne Huang, SWIFT; Natalie Zhang, SWIFT; Lin Su, The Agricultural Bank of China.

TORONTO

16 - 19 Oct 2017

Sibos is the premier annual event for the financial services community. The conference and exhibition are organised by SWIFT, and facilitate debate, networking and collaboration around the future of payments, securities, cash management, trade and financial crime compliance.

For one week every year, Sibos connects some 8,000 business leaders, decision makers and thought leaders from financial institutions, market infrastructures, multinational corporations and technology partners.

Sibos takes place in Toronto in 2017 as Canada celebrates its 150th anniversary.

For more information please visit www.sibos.com

@Sibos, #Sibos

linkedin.com/company/Sibos