CELENT

IMPERATIVES FROM SIBOS 2018: FINANCIAL CRIME COMPLIANCE

NEED FOR NEW TECHNOLOGY AND APPROACH FOR THE NEW DIGITAL ERA

Arin Ray
December 2018

This report was commissioned by SWIFT, which asked Celent to highlight the discussions at Sibos 2018. The analysis and conclusions are Celent's alone, and SWIFT had no editorial control over report contents.

OLIVER WYMAN

CONTENTS

INTRODUCTION

Every industry has its key event, where everyone involved comes together to discuss important issues of the day and drive business. For transaction banking and payments, that event is Sibos. Indeed, many people in the industry only attend this single event. Therefore, to describe it as a conference and exhibition does it a disservice, because for many it's the most important source of leads, learning, and intelligence for their year.

Celebrating its 40th year in 2018, Sibos traveled around the world, reflecting the global nature of both the event and the business it represents. This year the event was in Sydney, returning for a third time (the last being in 2006), and moving from last year's venue Toronto. Despite the pressures on both time out of the office and attendance at an international conference, SWIFT reports that over 7,500 registered for the event from over 150 countries. Attendees had the opportunity to meet with over 210 exhibitors and hear more than 450 speakers.

This is one of three reports that SWIFT has commissioned Celent to write — covering payments, cybersecurity, and financial crime compliance — and highlights the discussion at this year's Sibos, both on stage and in the many meetings that took place over the course of the week. Each report provides a summary of the key takeaways on the three themes, and we have weaved many strands together to bring out the bigger picture, and why this matters to the industry. It should be noted that the reports reflect the opinions of Celent and not those of SWIFT.

FINANCIAL CRIME COMPLIANCE: UNDER RENEWED SCRUTINY

Recent revelations of money laundering cases involving major banks are the latest but unfortunately not the least examples of the growing pain and severe consequences of lax control in financial crime compliance (FCC) operations. Therefore, it was not a surprise to see that financial crime compliance was again a major theme at this year's Sibos. It not only highlights the growing challenge for banks in FCC but also emphasizes the need for industry dialogue, collaboration, and knowledge sharing that can be facilitated through such an industry forum. This report highlights takeaways from numerous Sibos sessions and interviews relating to fighting financial crime such as sanctions, money laundering, terrorist financing, and fraud. A separate report highlights takeaways from sessions relating to cybersecurity.

REIMAGINING FINANCIAL CRIME COMPLIANCE FOR THE DIGITAL AGE

Digitalization is transforming the banking and payments landscape by creating new channels, providers, and alternative modes for funds transfer. However, the speed of innovation in the front office is not always matched by upgrades in operational risk controls and frameworks in the mid-office that are essential for tackling financial crime. Diminishing latency of payments processing, fragmentation of providers and channels, and constantly evolving regulations create technological challenges, especially in critical areas such as sanctions screening because sanctions are increasingly used as a tool for conducting foreign policy. Technology is enabling criminals to become more sophisticated and leverage emerging tools and new channels to evade traditional controls and oversight.

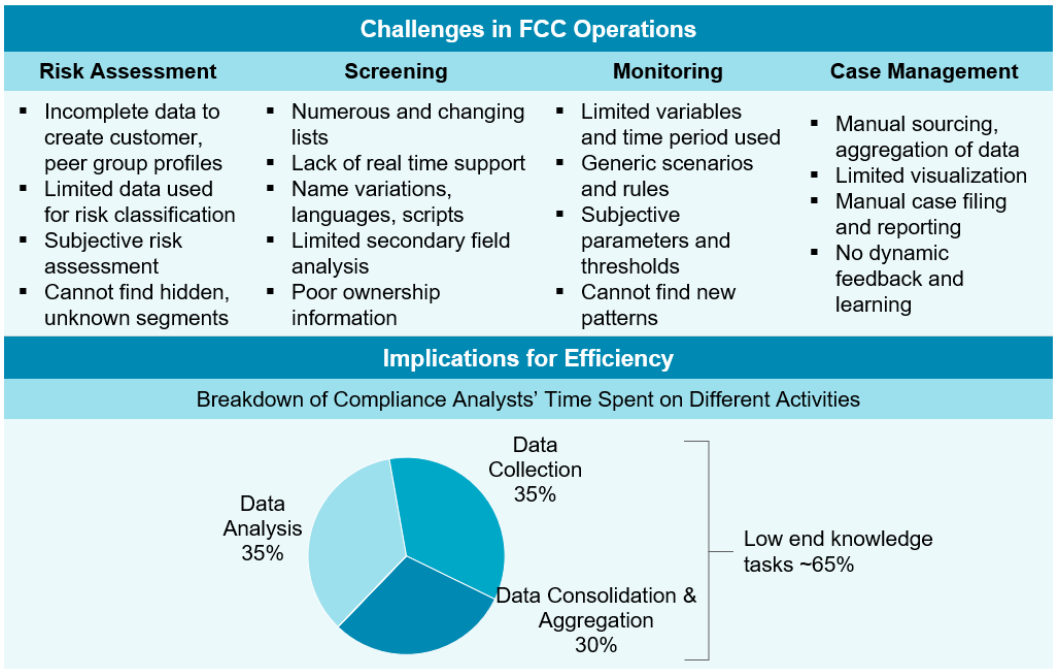
The speed vs. security dilemma is exacerbated by the fact that existing regulations are often inadequate for dealing with risks emerging from new players and business models such as money services, e-commerce, stored value providers, mobile wallets, cryptoassets, gig economy, and alike. As a panelist in the session *The digital revolution: Managing the emerging AML and regulatory risks* noted:

"Do we need to monitor a purchase of coffee? Probably no, but at what point does it become important?"

Regulators have started to rethink their approach. Some are considering focusing their supervisory framework along functional lines instead of types of institutions. So, they are considering uniform requirements for a product or service regardless of whether it is provided by a universal bank or a fintech. Concerns are emerging around cryptoassets that come with anonymity challenges; this can be ominous from a financial crime perspective if this asset class becomes prevalent.

Siloed operations and rules-based technology are ubiquitous in FCC operations, and they heavily rely on human intervention, compounding the severe operational challenges in FCC highlighted in Figure 1. The result is most banks have built up armies of compliance professionals, running into thousands at large banks. Yet, as can be seen from Figure 1, close to two-thirds of compliance analysts' time is spent on doing low level knowledge work such as data extraction, aggregation, and reporting. Not surprisingly, costs and complexities of FCC programs are becoming unsustainable.

Figure 1: FCC Operations Made Inefficient by Technology and Operational Challenges



Source: Celent

Securing the Securities Industry

With the spread of criminal activity into other segments, the securities industry is coming under greater scrutiny because it generates large volumes and value of money transfers. Today securities messages contribute to over half of total traffic carried over the SWIFT network, and recent analysis shows that the securities business of SWIFT's customers represents at least 30% of payments traffic. The securities industry is particularly vulnerable to attacks because it has many entry points, such as brokers, exchanges, clearing houses, custodians, and depository institutions. Traditionally securities market participants have conducted due diligence only on their clients and trusted their partners for compliance downstream. That approach is proving to be inadequate with participants being expected to know all counterparties in the complete transaction value chain. The challenge is similar to that faced by correspondent banks, but there are nuances specific to the securities industry such as omnibus account structure, collective investment

schemes, definition of beneficiary owner, complex multiple jurisdictions, and associated legacy technology complexities.

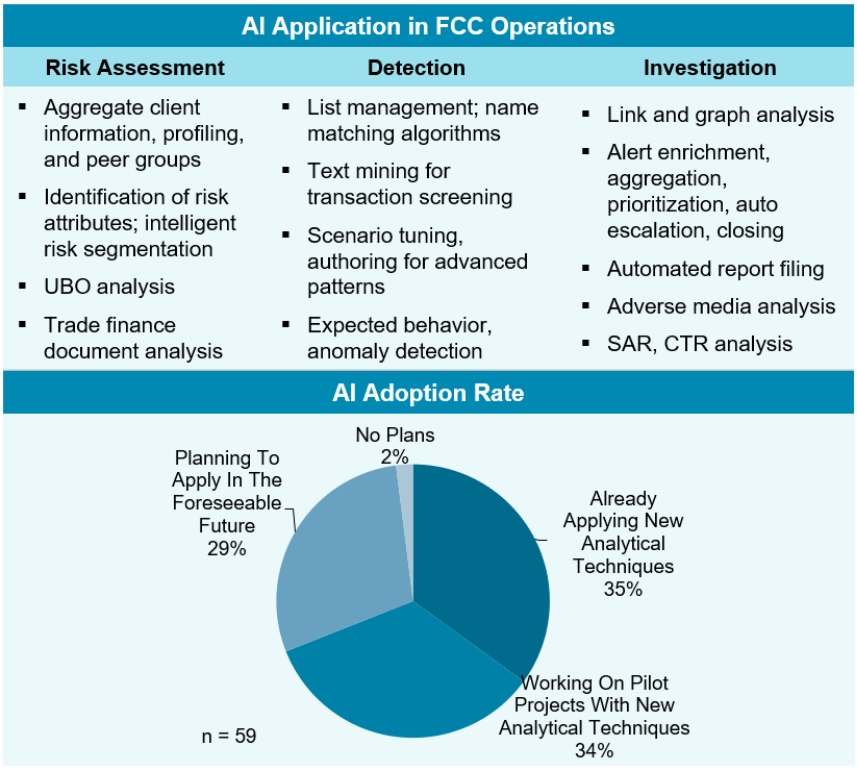
The industry lacks regulations and guidelines addressing these specificities. A group of global banks that together account for an overwhelming share of cross-border securities intermediation has been working with the International Securities Services Association (ISSA) to formalize standards- and risk-based principles, and is currently in the process of finalizing the principles and communicating them to the wider markets, after which they expect the implementation phase to commence. It is noteworthy that the intergovernmental body Financial Action Task Force (FATF) adopted a risk-based approach for the securities sector in its October 2018 Plenary, and outlined the key principles involved in applying a risk-based approach for fighting financial crime in this sector.

Artificial Intelligence for Solving Real Problems in FCC

High costs and large team sizes in FCC are primarily due to growing alert volumes, of which an overwhelming share are false positives, as was confirmed by many panelists. Some mentioned that routine tasks to resolve the alerts cause "analyst fatigue" that can result in suboptimal decisioning — the costs of non-compliance and missed true positives can be significant as well. As the industry transitions into the new digital era, there is a dire need for intelligent automation across the FCC value chain.

New technology such as robotic process automation (RPA), artificial intelligence (AI), and machine learning (ML) is paving the way for much-needed transformation in compliance. The new tools and techniques can analyze large volumes and different types of data, offer actionable insights in real time, and drive efficiencies through automating manual tasks. Machines can identify unknown patterns, such as in client segments, peer groups, transactional behavior, or a network of entities.

Figure 2: AI Adoption Is Underway in FCC Operations



Source: Celent (upper panel), Institute of International Finance (lower panel)

Several of these tools are already being tested such as natural language processing, identity resolution, graph analytics, cluster and pattern analysis, and anomaly detection. Celent has seen numerous applications of them, as highlighted in Figure 2.

- Risk assessment and segmentation is improved by applying cluster analysis to find client segments with similar risk profiles. Dynamic updates based on clients' evolving behavior and profile information can aid up-to-date monitoring.
- Big data analytics help create a 360-degree customer view encompassing multiple accounts, addresses, phone numbers, devices, geospatial information, and so on.
- Screening efficiency is improved through intelligent automation in data normalization, free text analysis, keyword searches, and context-based linguistic analysis.
- Data-driven approach is being used in transaction monitoring to fine-tune existing rules and scenarios, and author new typologies and scenarios using pattern analysis and anomaly detection. Big data analytics allows banks to move away from transaction- or account-based to peer group, network based, and holistic monitoring.
- Case management and investigation is seeing efficiency improvements through widespread adoption of RPA as well as advanced analytics for enriching, categorizing, prioritizing, and correlating alerts and events.

Celent sees early adoption of these tools to be tactical and used for enhancing and augmenting existing systems rather than replacing them.

As Far as AI Can See

Adoption of these new tools and technology is well underway. A survey of 59 financial institutions conducted by the Institute of International Finance found that 35% of respondents are already using advanced analytical tools and techniques in FCC, with an additional 34% currently working on pilots (see Figure 2).[1] The solution provider landscape is maturing fast, as was noted by a panelist in the session *The future is now: Integrating new technologies (AI and Robotics) and financial crime compliance:*

"Two years ago we were asking for use cases when consultants were telling us the benefits of AI and ML and there were no use cases, and now there are many ready solutions."

A panellist from a global bank mentioned in the session *Reconciling real-time payments with financial crime and fraud controls* that close to 50% of payment screening alerts are now being resolved with the help of AI. Celent has seen significant benefits from several AI use cases; examples include reduced volume and better quality of alerts, over 30% reduction in false positives, over 40% low touch closing of alerts, over 25% improvement in investigation efficiency, multimillion-dollar cost savings per year, identification of previous undetected false negatives, more holistic approach in compliance, and so on.

Data is the fuel driving analytics, so data quality, transformation, and governance issues will be critical in their adoption. A major challenge cited by multiple institutions related to the dilemma between data privacy rules and the need for holistic monitoring. Banks need aggregate data cutting across business lines and geographies for comprehensive analysis, yet regulations can prevent them from sharing within or between institutions.

Perception of black box and need for explainability of AI models came up in several discussions. Practitioners emphasized that these challenges are use case-specific, and not prohibitive if decisioning is overseen by analysts. Issues about model governance and regulatory response to AI elicited murmurs, but it was evident that regulators are generally supportive of the developments and are closely following them.

[1] *Machine Learning in Anti-Money Laundering*, Institute of International Finance, October 2018

Another challenge cited was the dearth of expertise; it is not easy to train and retain staff with expertise across technology, regulations, investigations, and local language skills, and a banker noted that *"the war for talent is real."* Participants therefore felt there is a need to democratize new technology by making it more user-friendly and easily consumable by business users — a trend Celent has seen among many vendors.

Need for Partners Against Crime

Even if financial institutions overcame their internal limitations, individually they will still have only a partial view and knowledge of the complex web of criminal activities because crime spans across many intermediaries in the transaction value chain, with each having different risk appetites, and disparate risk management standards, frameworks, and practices. Therefore, individually they can miss the bigger picture, and regulators can lose the forest for the trees based on the isolated reports coming from these institutions.

Information and knowledge sharing in financial services is currently limited due to restrictive rules and practices. There is a need for more dialog within an institution (such as product and compliance departments, sister organizations, across geographies) and between institutions for sharing information, best practices, learnings, and insights. Many panelists felt more collaboration with fintechs will be mutually beneficial because fintechs can bring in more data, insights, and analytical capabilities, and learn from financial institutions' knowledge and expertise with risk regulations and FCC operations.

There is also a desire for more participation and inputs from regulators for harmonizing disparate regimes, setting standards and practices especially involving emerging technology, providing feedback to filed reports, and generally guiding banks to see the bigger picture. Regulators shared this view as well and highlighted the need for public-private partnerships and financial information sharing partnerships in the sessions *The future is now: Integrating new technologies (AI and Robotics) and financial crime compliance*, and *Partners against crime: Public-private partnerships, big data and the sharing economy*. Some such initiatives are already underway, but more needs to be done. Panelists in multiple sessions, such as *The digital revolution: Managing the emerging AML and regulatory risks*, and *Partners against crime: Public-private partnerships, big data and the sharing economy,* expressed the desire to see law enforcement agencies involved in these efforts.

Sharing Is Caring

There is a growing demand for collaboration and sharing the operational burdens in FCC, especially given all banks must undertake significant efforts which are similar in nature and therefore are highly redundant for the industry — these only add to the cost without providing any competitive edge. Panelists in the session *Partners against crime: Public-private partnerships, big data and the sharing economy* felt the industry as a whole can benefit through mutualization of efforts. We have seen utilities and shared services for KYC data, including SWIFT's KYC Registry for correspondence banking. There is now a desire to move up the chain and mutualize other FCC parts; examples cited included SWIFT's sanctions application shared service, or a hypothetical central collective transaction monitoring for multiple banks. One participant from a bank noted:

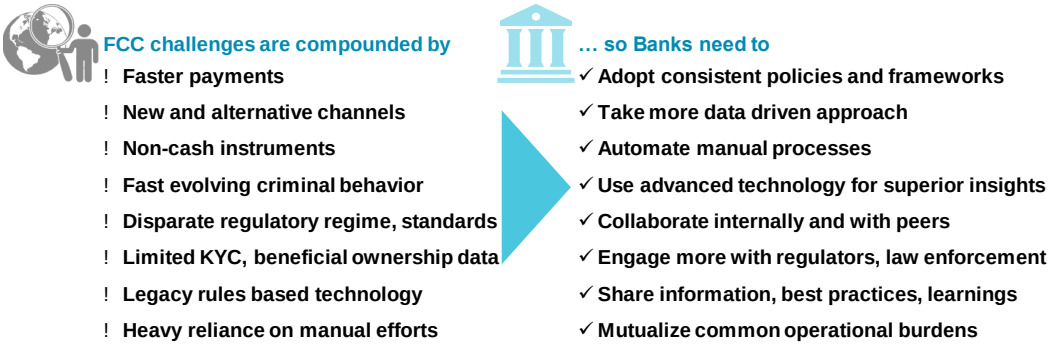
"The idea is to do it once centrally and do it in a standardized way."

The examples of the auto and aviation industries were brought up to highlight the need for sharing and outsourcing non-core parts. Even within financial services there is a strong desire to mutualize costs of functions that are non-competitive, with FCC operations being a prime example. Creating utilities is not always easy, and will require banks, service providers, and regulatory agencies to work together and share the costs and operational burden. It was noted that new technology like blockchain with secure and consensus-based sharing framework could be of immense help in such efforts, especially in information and identity sharing and management.

THE PATH FORWARD

Compliance professionals feeling fatigued by the onerous burdens were reminded of the maxim from the former US Deputy Attorney General Paul McNulty: "*If you think compliance is expensive, try non-compliance.*" The good news is that new technology can help overcome the challenges but will require concerted thinking and action.

Figure 3: Enhancing Efficiency and Effectiveness in FCC



Source: Celent

Banks need to strengthen operational controls and dismantle internal silos and fragmented architecture for holistic compliance. Specifically, data management and governance will be critical because promises of new technology can only be realized on the back of clean and accurate data. Technology providers should facilitate ease of adoption by developing solutions that are easy to understand, document, and use.

Regulators have an important role to play in improving compliance standards in the industry. Regulatory fragmentation can create arbitrage, thereby allowing criminals to attack the system through its weakest links; therefore, strengthening regulations for emerging segments and channels, and harmonizing disparate regimes and conflicting regulations will be important. As some panelists noted, real-time screening and real-time payments are incongruous if there is no mechanism for freezing or repatriating funds. Similarly, requiring banks to achieve 360-degree customer views is unrealistic with onerous data privacy requirements. "*Financial institutions should not have to choose which regulations they want to violate,"* one compliance professional observed.

Financial institutions noted that there is sometimes over-reliance on regulators to show the way, making banks reactive in compliance. This mindset needs to change. The industry needs to find more ways to collaborate, and regulatory backing to industry efforts will help overcome barriers and accelerate adoption. Sibos is a fertile ground for the industry to collaborate, find common ground, and debate differences. Sibos 2018 has planted the seeds for new ideas, and nurtured existing ideas that the industry has been discussing. It is now time to put the ideas into action. With the shadows of Brexit looming large, few can predict what the world will look like when Sibos reconvenes in 2019 in London, but one thing is certain — financial crime will not go away, and financial crime compliance will continue to be a pressing issue for the day.

Many of the issues highlighted in this note are discussed in greater detail in Celent research as noted in the Related Research section at the end of this report. Celent will continue to track the developments and inform the industry debate in this critical area.

Was this report useful to you? Please send any comments, questions, or suggestions for upcoming research topics to info@celent.com.

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

SUPPORT FOR FINANCIAL INSTITUTIONS

Typical projects we support related to risk management and compliance include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes, particularly in risk management and compliance. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

SUPPORT FOR VENDORS

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials — including your website and any collateral.

RELATED CELENT RESEARCH

Enhancing AML Efficiency and Effectiveness: Artificial Intelligence Transforms the Rules of the Game
October 2018

Fighting Financial Crime Amidst Growing Complexity: The Need to Rethink AML Technology and Approach
October 2018

Evolution of Utilities and Managed Services: From Cost Control to Innovation
May 2018

Achieving Integrated GRC in an Interconnected Digital Age
May 2018

AI Made to Reduce False Positives, Part 1: Detection Capabilities and Use Cases
May 2018

Achieving Holistic AML: Focus on Watchlist Screening
March 2018

Innovations in AML and KYC Platforms: New Models Powered by Advanced Computing
January 2018

Innovation in AML Technology: New Tools for Optimizing Compliance Efficiency
November 2017

A New Era in Capital Markets Surveillance: As Far as the AI Can See
November 2017

Cloud-Enabled Governance, Risk, and Compliance Solutions
October 2017

Under the Spotlight: Innovative Vendors in Financial Crime Case Management Technology
August 2017

Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency
August 2016

Emerging Solutions in Anti-Money Laundering Technology
May 2015

Emergence of a Utility Model: The Case of KYC On-Boarding Solutions
September 2014

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

For more information please contact info@celent.com or:

Arin Ray aray@celent.com

AMERICAS

USA

200 Clarendon Street, 12th Floor
Boston, MA 02116

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Av. Doutor Chucri Zaidan, 920 –
4º andar
Market Place Tower I
São Paulo SP 04578-903

Tel.: +55.11.5501.1100
Fax: +55.11.5501.1110

EUROPE

France

1 Rue Euler
Paris
75008

Tel.: +33.1.45.02.30.00
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059