CELENT

IMPERATIVES FROM SIBOS 2018: CYBERSECURITY

EDUCATION, DISCIPLINE, AND COLLABORATION

Joan McGowan and Gareth Lodge
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, as for many it's the most important source of leads, learning, and intelligence for their year.

Celebrating its 40th year in 2018, Sibos has travelled around the world, reflecting the global nature of both the event and the business it represents. This year the event went to 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 — on payments, cybersecurity, and financial crime compliance — to highlight 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.

CYBERSECURITY: FRONT AND CENTRE, A CONCERN FOR EVERYONE

The cybersecurity report does not touch on AI and advanced technologies available to the financial services industry to help in the fight against cybercrime — these, of course, are critical to overcoming the current operational challenges faced by most every institution and are covered in the sister reports. Instead, this report focuses on new threats, challenges, and the immediate need for improved cybersecurity through education, discipline, and collaboration, all of which were headlined throughout Sibos.

OPENING THE DOOR TO CYBER RISK

A key theme of Sibos 2018 centred on the powerful drivers of change within the financial services industry: evolving customer needs, open banking regulations, compliance requirements, and advances in technology. We are watching the industry morph into an open marketplace with new players, new products, and new ways to distribute.

While the changes position the industry to compete in a thriving and open marketplace, the drivers of these changes are also enablers of fraud. The industry is opening up to new levels of industrial-scale attacks — attacks that operate beyond traditional system silos, institution perimeters, peer groups, and accounts. A future large-scale cyberattack on financial infrastructure will very likely cause a significant and potentially systemic impact for the industry as a whole.

Figure 1: Financial Institutions Open Doors to Cybercrime and Disruption

Source: Celent

The Sibos tracks debated seven megatrends, illustrated in Figure 1, mainly with an eye to the profound changes and opportunities they bring to the industry. This report purposefully focuses on the trends as enablers of cybercrime and looks at the new threats and challenges that the transaction banking and payments industry faces.

The threats described below were raised across the different tracks, sessions, panels, and keynote speeches and were front and centre for all concerned.

1. **Globalisation:** Economic globalisation brings with it increased cross-border payments, greater volumes of transactions, and a growing and more open threat landscape that creates new possibilities for cybercriminals to intercept and commit fraud. Globalisation is shaping opportunities for illicit transfers of funds and money laundering, involving local and transnational networks.

2. **Customer expectations and digitisation:** Our expectations as online banking customers are high. We are used to getting easy access to online providers — and we naturally expect financial institutions to be able to keep up. But for the majority of institutions, it is a strategy that is still in-flight and that requires a fundamental pivot from a slow, risk-averse, and incremental approach to an agile offering of immediate services and digital applications. Balancing expectations and security remains a concern for the industry and, adding to the potential threats of forgoing security for ease of use, is the general cyber ignorance of consumers as they escalate their daily digital engagement.

3. **Open banking:** The EU's Payment Services Directive version 2 (PSD2) legislates that financial institutions open up the banking industry to trusted third parties, leading to a greater inherent risk of sharing data across a wider and unregulated ecosystem. Plus the use of application programme interfaces (APIs) to connect to third parties exposes an institution's attack surface to malicious users such as malware coders

and website and mobile API hijacking. As a newer technology, APIs bring unknown risks, specifically around authentication management.

4. **Faster payments:** The push to real-time or faster payments puts more pressure on institutions to flag suspicious transactions in milliseconds, because once the funds have left the institution, the transaction is irrevocable. Most institutions' systems are not set up to move this quickly. If a fraudulent payment is detected, faster payments schemes offer little time to recover the funds by recalling the transaction or freezing the end beneficiary account. Faster payment transactions also put more pressure on logins and password security and make it easier for criminals to scam login details and break into accounts.

5. **Fintechs and innovation:** Firms focused on introducing AI technologies are transforming the criminal economy as dramatically as they are every other part of our economy. AI has become an "arms race" between defenders and attackers — attackers lead.

   For example, "*Crimetech"* providers are deploying advanced technologies in the cloud to efficiently scale attacks to target millions of systems, and attacks are automated to require minimal human involvement. The industry must be willing to adopt similar technologies to have any chance in stopping nation states, organised cybercrime, hactivism, cyber terrorism, and economic espionage.

6. **Regulations:** With the potential for punitive fines for noncompliance, most institutions' immediate response to General Data Protection Regulation (GDPR) and PSD2 has been to focus narrowly on the required compliance processes; as such they have underestimated the operational challenges of the legislation.

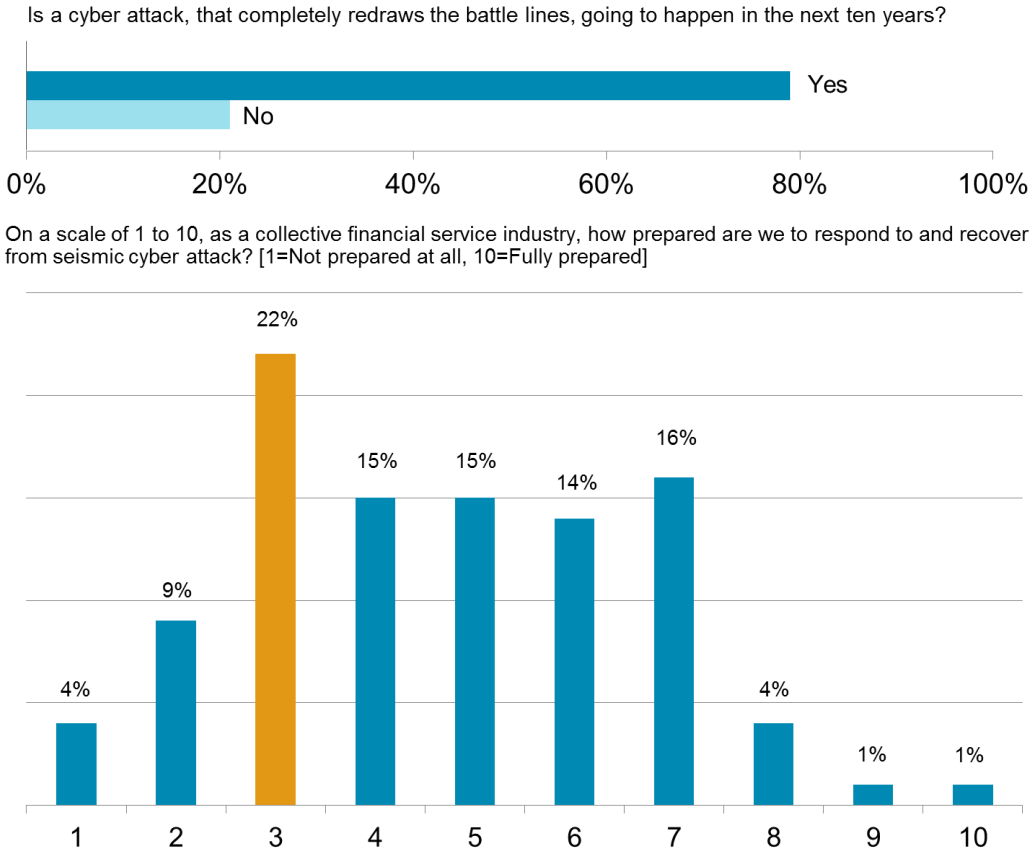
   Such new regulations, compliance complexity, explosive data requirements, poor incumbent data quality, and a focus on compliance at the expense of other priorities will only empower criminals to a higher level of anonymity as they move around the ecosystem with greater impunity. Furthermore, the sheer number of emails to attain GDPR data consent requirements has significantly increased the threat vector for email scams and identity theft.

7. **Cryptocurrencies:** We're a long way from reaching consensus on whether to embrace cryptocurrencies or how to approach and regulate such currencies. But we know the intentional design of cryptocurrencies is to ensure anonymous (or at least pseudo-anonymous) transactions that do not rely on a third party like a bank. There is little to no personally identifiable information transmitted in a transaction itself, and currencies are easily monetised into cash. This level of anonymity makes cryptocurrencies an ideal exchange for transacting illegal activities — such as tax evasion, black market transactions, financing terrorism, avoiding sanctions, and enabling ransomware payments and money laundering schemes.

WAITING FOR A SEISMIC ATTACK

On day 2 of Sibos the question was posed in the main cyber track: *"Is a seismic attack inevitable?"* The resounding answer from the panel and audience poll question was *"Yes."* Figure 2 shows the percentage response to this question and to the question of how prepared the industry is to respond to a seismic attack. As the results show, we are not close as an industry to being prepared for a black swan event.

Figure 2: Sibos Cyber Session Is a Seismic Attack Inevitable? Poll Questions



Source: Sibos 2018 "Is a 'cyber 9/11' event inevitable?"

The worst imagined scenario described by the panel of experts will be either an orchestrated Distributed Denial of Service (DDoS) attack or an orchestrated ransomware attack.

According to the panel, *"Coordinated DDoS attacks against the biggest institutions will lead to a run on banks, a systemic liquidity crisis, and a fall out of disastrous proportion."* A WannaCry-type ransomware attack, as was seen by the UK's National Health System in May 2017, is one of a new generation of self-propagating threats that fly under the radar and, again according to the panel, *"If the world's financial systems are held to ransom the effect on global banking will be seismic."*

Another scenario described by the panel is an attack by a rogue nation or terrorist group on financial institutions. Inside North Korea, for example, the Lazarus Group, (also known as Hidden Cobra) routinely looks for ways to compromise financial institutions and exploit cryptocurrencies. An attack on a bank, investment fund, custodian firm, ATM network, SWIFT, or the Federal Reserve itself would represent a direct hit on financial services systems.

The capacity of organised crime is increasing two-fold each year and, according to analysis by Oliver Wyman, cybercrime alone cost nations more than $1 trillion in 2017.

Cyberattacks are the biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks.[1]

Cybercrime has become a high-performing industrialised business. Organised criminals operate across jurisdictions with a P&L management structure that includes organised markets, exchanges, cryptocurrency payments and rapid monetisation, specialist operators, administrators, data scientists, insiders, outsourced service providers, and integrated supply chains. The threat has moved to advanced, persistent unknown attacks. Therefore, institutions must shore up their defences by monitoring the growing ecosystem and becoming more resilient to threats by improving response and recovery capabilities.

Securities Market Threat Level at Red

The securities market moves trillions of dollars every day, and securities messages account for over half of total traffic carried over the SWIFT messaging platform. Recent analysis also shows that the securities business of SWIFT's customers represents at least 30% of payments traffic. These funds are typically of high value, and cybercriminals know this: it can be only a matter of time before we see a large-scale, organised cyberattack against the securities market.

Any belief that a closed environment and highly complex fund transactions within capital markets will discourage cyber hacks is unfounded. The market involves hundreds of partners; operating models are diverse and disjointed, and the ecosystem has multiple entry points. A perfect environment to hide in plain sight. In the cyber session titled *"Cyberattacks in the securities market? Hold on, I thought it was just a payments problem …"* the panel expressed fear that it is highly likely there is an organised criminal gang already within the securities ecosystem.

> "It is highly likely there are organised criminal gangs already within the ecosystem, watching the workings of the market, learning the processes, and ready to move when the time is right."

Governments have recognized that capital markets are a promising and probable next target for cybercriminals and are currently legislating to improve security capabilities and response and recover mechanisms across the markets. Industry associations, such as the International Securities Service Association (ISSA), have cybersecurity as their number one priority. ISSA's cybersecurity working group recently published three cybersecurity papers that prescribe a pragmatic approach to security through education, intelligence collaboration, and sharing best practices. Learning from other markets that have suffered large-scale attacks will greatly progress the effectiveness of a resilient cybersecurity program. For instance, ISSA is working with SWIFT to improve cybersecurity hygiene by tailoring best practices based on SWIFT's Customer Security Programme (CSP).

Collaboration Is an Imperative of Cybersecurity

A key message speakers conveyed during this year's cyber sessions was the imperative for collaboration across the industry. Understanding the motivation, context, and tactics of bad actors will be made a lot easier by sharing intelligence.

The power of intelligence sharing brings many benefits:

- Correlation of indicators of compromise (IOCs) across institutions that otherwise would remain hidden.

[1]https://www.oliverwyman.com/our-expertise/insights/2018/sep/how-a-cyber-attack-could-cause-the-next-financial-crisis.html

- Learnings from other institutions and other industry sectors.
- Greater situational awareness of targeted campaigns and other security issues.
- Shared best practices from identification through remediation.
- Proactive defence strategies through access to more comprehensive, real-time threat information.
- Rapid communications to customers of potential incidents and attacks.
- Cost savings from reduced duplication of efforts and shared skill sets.

Even with such obvious motivations to share, the audience acknowledged that few of them have invested in the necessary data analysis and integration technologies required to exchange intelligence in a meaningful way.

An example of a robust sharing platform for the payment sector is SWIFT's Information Analysis and Sharing Centre (ISAC) portal, established in May 2016. The platform enables the sharing of threat intelligence concerning incidents involving SWIFT customers. For instance, ISAC collates and shares information about malware details, file hashes, YARA rules, and IOCs, as well as details on the modus operandi used by the cybercriminals. The intelligence is collected and shared in an anonymised format and made available to SWIFT customers. The community also partners to reinforce security across the SWIFT infrastructure, through SWIFT's CSP, which is covered in the next insight on cyber risk education.

Protecting Smaller Institutions

The theme of intelligence sharing was also presented in two well-attended sessions on protecting the long-tail of smaller institutions from cyberattacks. Smaller institutions are less likely to belong to an information-sharing organisation than larger institutions, because they lack the resources and tend to prioritise efforts on internal systems and processes. However, a breach of a local bank may have a far greater knock-on effect on the global market, as we continue to lessen the degree of separation.

Thwarting cyberthreats is a goal that can only be reached by the collective objectives of a shared industry that is inclusive, endorses a cyberthreat intelligence sharing community platform, agrees language and exchange standards, and shares best practices with private and public partners including government, law enforcement agencies, universities, and cyber intelligence vendor specialists.

The collaborative model could be the industry's strongest weapon in abating large-scale, new cyberthreats.

Education, Education, Education

There are other practical means for financial services firms to reduce the likelihood of a major cyberattack. Speakers across sessions echoed each other's opinions in recommending that institutions maintain a high state of cyber hygiene and cyber education.

Humans are prone to errors and misjudgement, and it is only through awareness, education, and discipline that errors and, therefore, threats can be reduced. In particular, our inability to spot phishing emails time after time is (un)impressive. The FBI reported a 136% increase in losses related to business email compromise attacks from December 2016 to May 2018. A spoofed email of high importance from an executive asking a subordinate to transfer funds into an account is rarely going to be questioned. Another stubborn miscalculation is the continued failure to carry out timely patches to software.

This is a hard one to fathom, because patching vulnerable software, if implemented consistently, would stop most hackers cold and significantly reduce risk.

> ***" … inadvertent insiders were responsible for more than two-thirds of total records compromised in 2017." IBM X-Force Threat Intelligence Index 2018***

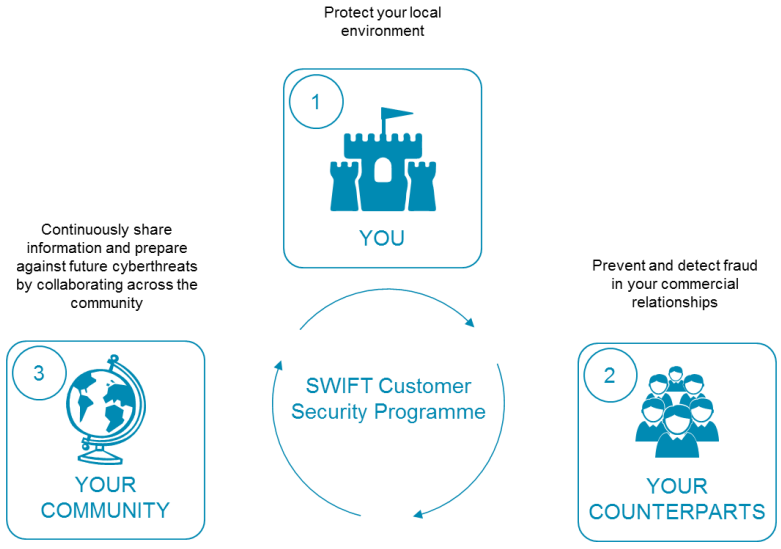
According to the IBM X-Force Threat Intelligence Index 2018, inadvertent insiders were responsible for more than two-thirds of total records compromised in 2017. More than one-third of inadvertent activity experienced by X-Force-monitored clients involved attackers attempting to trick users into clicking on a link or opening an attachment.[2]

Education needs to start with the Board and C-Suite and the recognition that at some point your organisation will be attacked. Leadership must take on responsibility for the implementation of a consistent and rigorous cybersecurity program that involves culture awareness, willingness to share intelligence, and continuous education.

Awareness should not be an issue. The industry has witnessed some of the largest attacks to date, but turning awareness into a daily discipline is far from pervasive. The industry must share lessons learned and methods of mitigation. A good example of such practice is the work SWIFT is doing with securities market CISOs to help develop more robust cyber policies and controls, based on SWIFT's security programme (CSP).

SWIFT's CSP addresses cybersecurity hygiene through best practices and self-attestation to those practices. The programme's overall objectives are to secure and protect customers' local environments, prevent and detect fraud in their counterparty relationships, and to work together as a community to prevent future cyberattacks. Figure 4 outline's SWIFT's objectives to reinforce cybersecurity across institutions, partners, and the payment's industry.

Figure 4: Swift Customer Security Programme Objectives Are to Reinforce Cybersecurity Across Institutions, Partners, and the Industry



Source: Celent

[2] https://www.ibm.com/security/data-breach/threat-intelligence

Knowing that parties have implemented SWIFT's mandatory and advisory security hygiene controls will provide institutions with a level of comfort that other entities are practicing the same discipline of strong cybersecurity. Combining CSP with SWIFT's sharing initiative — SWIFT ISAC — will further strengthen defences through the exchange of meaningful IOCs and trend intelligence across the banking transaction and payment's sector.

The time given over to cyber risk at Sibos 2018 was notable and reflects the concerns of the industry. The changes happening across the industry are unprecedented, and we may well look back and consider the past ten years of profound, structural change to risk management a mere upgrade compared to what's coming. These changes will bring an abundance of opportunities and an abundance of threats.

THE PATH FORWARD

Despite the transaction banking and payments industry being built upon co-operation between institutions, there are few places other than Sibos where the industry gathers to discuss what is happening and on such a global scale. Given the changing needs of the market, the shifting position of its players, and how increasingly important it is to think globally, it should come as no surprise that now more than ever, Sibos remains a key event for the industry.

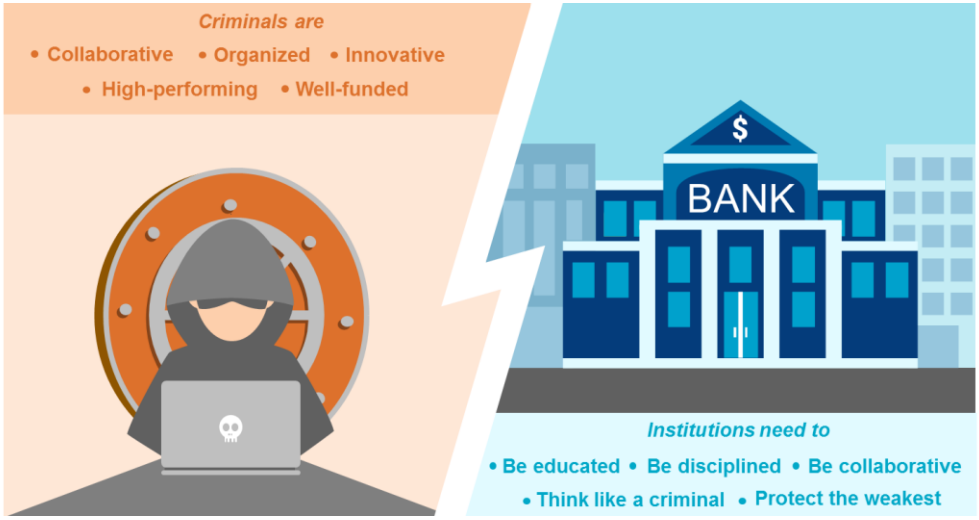
So what should industry players expect or do before they reconvene next year? The very location of the host city, London, is perhaps symbolic of the upheaval and uncertainty the financial services industry will face in a post-Brexit world. In the area of cybersecurity, it was good to hear one voice echo the need to better prepare for highly sophisticated, large-scale, and new types of cyberattacks.

The industry must act together to:

1. Significantly improve daily cyber hygiene routines and overall cybersecurity practices. Human errors are the greatest threat to an organisation but the easiest fix.
2. Be better educated about changing tactics, techniques, and share lessons learned.
3. Collaborate and share IOCs in context and cyber intelligence trends in a timely manner and far more widely.
4. Defend the entire ecosystem — the weakest links are likely outside of your institution.

We can learn from the world of cybercriminals — they are well-organised, willing to share their trades, and perform as high-functioning businesses capable of operating globally. It is our responsibility to work with a greater sense of urgency, to develop a higher level of sophistication, and to collectively mitigate the more menacing cyberthreats the industry faces.

Figure 5: Cybercriminals Are on the Attack, the Financial Services Industry Is on the Defence



Source: Celent

Many of the issues and developments covered in this report have been discussed in greater detail in Celent research reports, 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 risk management and cybersecurity:

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 cybersecurity and risk management across financial services. 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 analyse 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

Combatting Financial Crime at Scale: With a Coordinated, Intelligent, Real-Time Response
October 2018

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

Robotic Process Automation in Risk and Compliance
August 2018

AI Made to Reduce False Positives Part 2: Vendor Spectrum
July 2018

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

Claims Fraud Detection Systems: 2018 IT Vendor Spectrum
May 2018

Achieving Holistic AML: Focus on Watchlist Screening
March 2018

Risk Management and Compliance 2018: CROs Navigate NextGen Tech
May 2018

The Greatest Risks Impacting Treasury and Finance Organizations
February 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

Financial Crime Mitigation in the New New World of Blockchain
October 2017

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

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

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

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

Joan McGowan jmcgoan@celent.com
Gareth Lodge glodge@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