CELENT

THE MIGRATION PATH TO NEXT GENERATION KYC-CDD

Neil Katkov
May 2019

This report was commissioned by NICE Actimize, which asked Celent to design and execute a Celent study on its behalf. The analysis and conclusions are Celent's alone, and NICE Actimize had no editorial control over report contents.

OLIVER WYMAN

CONTENTS

EXECUTIVE SUMMARY

KEY RESEARCH QUESTIONS

1 *What are some of the key challenges in KYC-CDD processes?*

2 *Which new technologies can support more efficient KYC-CDD processes?*

3 *What factors are supporting the adoption of next generation KYC-CDD technology?*

Know your customer (KYC) and customer due diligence (CDD) requirements are the most burdensome areas of anti-money laundering (AML) compliance for many firms. Because KYC-CDD processes are central to onboarding and understanding customers, they are also arguably the most strategic area of the AML compliance chain.

Increased speed and efficiency in KYC-CDD is sorely needed to reduce the operational burden of compliance and to support the faster pace of digital financial services. New regulation such as beneficial ownership requirements put additional pressure on AML compliance operations. Just in time, next generation technologies like intelligent automation are streamlining resource intensive KYC processes and bringing them into the digital age.

Financial institutions and other organizations are seeking new technologies to support modern AML compliance paradigms including holistic AML, risk-based customer segmentation, perpetual KYC, and KYC for digital services. Long KYC and onboarding cycles for corporate and institutional customers also call out for new solutions to provide relief.

- Intelligent automation can help automate KYC-CDD tasks including holistic, 360-degree customer views, entity resolution, compilation of customer profiles, and analysis of beneficial ownership structures.
- Advanced analysis of external unstructured data increases efficiency by automating labor intensive CDD processes and can identify relationships and risks that might otherwise go undetected.
- Artificial intelligence (AI) and machine learning can lead to reduction in false positives of 30% to 70% or higher as well as 25% to 40% improvements in investigation efficiency.
- Natural language generation (NLG) can automate the assembly of relevant case information into coherent narratives to support regulatory filings.

The focus of regtech on AML-KYC, AI initiatives by incumbent AML software providers, a growing track record of successful POCs and implementations, and regulatory initiatives supporting the use of next-gen technology for AML compliance are all supporting progress in KYC-CDD technology.

CURRENT STATE OF KYC-CDD

Key Research Question 1

What are some of the key challenges in KYC-CDD processes?

Customer identity and compliance checks, risk assessment and scoring, enhanced due diligence investigation, periodic customer reviews, and beneficial ownership analysis are among the major pain points leading to inefficiencies in KYC-CDD operations.

Know your customer (KYC) and customer due diligence (CDD) requirements are the most burdensome in anti-money laundering (AML) compliance for many firms. Because KYC-CDD processes are central to onboarding and understanding customers, they are also arguably the most strategic area of the AML compliance chain.

This holds true for both the retail and corporate side of financial services, as well as for digital financial services and online lifestyle services and e-commerce.

Retail banks and other personal financial services providers open large numbers of new accounts on a continuous basis and maintain exponentially larger pools of existing customers. KYC-CDD checks must be performed for both onboarding new customers and for periodic risk reviews of existing customers.

KYC-CDD processes are complex and demanding, even when seen from a high level, and each step in the process presents challenges.

- **Customer identity and compliance checks.** Preliminary screening of customers against identity verification databases and government watchlists, while straightforward in concept, has proven difficult in the execution.
  - Capturing name matches in the face of irregular or imperfect input data as well as intentional obfuscation by bad actors requires sophisticated matching algorithms, dictionaries, and token libraries, developed over years and requiring significant domain expertise.
  - To ensure adequate coverage of customer risk, customer screening may involve multiple official/government watchlists, commercial datasets such as PEPs, and other external data such as negative news.
  - Partly due to the need to spread a wide net in terms of these matching algorithms and reference datasets, compliance screening typically generates extremely high proportions of false positive alerts, often exceeding 90 or 95%. These false positives must then be reviewed and cleared by analyst teams, requiring significant time and cost. At the largest global banks, these teams can number in the 1,000s of employees.
- **Risk assessment and scoring.** Determining a customer's risk profile at onboarding involves completing a checklist of static attributes such as occupation, industry, and type of entity; as well as capturing information on intended or expected transaction frequency and size, counterparties, target geographies, and financial products.
  - This information is then scored according to a risk matrix created by the financial institution. It is also used to establish an expected activity profile, which can serve as a basis for flagging activity atypical of the expected behavior.

  - Compliance screening results, such as a PEPs hit, can also be used as a factor in the risk assessment.
  - Further complicating the process, insights gleaned from customer due diligence research into additional data sources (such as adverse media) should be reflected back into the risk score.
- **Enhanced Due Diligence (EDD).** Compliance screening alerts, high risk scores, and other red flags can lead to further investigation of a customer's background, associates, and activity.
  - EDD investigations are highly manual processes that involve performing searches on a wide range of data sources including industry databases such as fraud lists, government records such as bankruptcies and criminal actions, and open source intelligence (OSINT) sources such as negative news and social media.
  - Investigators compile their findings into reports combining quantitative and narrative information and, if warranted, file regulatory reports.
- **Periodic customer review.** In order to keep abreast of the current status of their customers, risk assessments of existing customers must be performed on a periodic basis.
  - The importance of periodic customer review cannot be overstated. Failure to perform these sweeping checks has exposed institutions to financial crime risk (money laundering, terrorist financing, and fraud); as well as regulatory action such as lookbacks.
  - The operational burden of customer review also cannot be overstated. The process involves all of the above KYC steps — compliance screening, confirmation of customer profiles and risk scores, and EDD when needed — across the entire existing customer base and at regular intervals.

CORPORATE KYC

KYC for corporate and institutional clients presents additional challenges, leading to longer cycle times for KYC processes.

- **Document collection.** Due diligence for corporate clients involves collection of articles of incorporation, business licenses, organizational charts, and other documents pertaining to the organization's business. While this can be a straightforward exercise for small enterprises, KYC on mid-market and larger corporations is more complex and can require documentation covering multiple divisions and regions.
- **Expected activity.** Corporate KYC may also require establishing the activity profile of an organization in terms of size, frequency, and type of transactions; cash flow and velocity; and counterparty types and regions.
- **KYC on Officers.** KYC on corporate clients involves identifying primary corporate officers and, furthermore, running separate KYC checks on them.
- **Beneficial ownership.** Recent regulations in the EU, United States, and other jurisdictions require identifying the individuals who are the ultimate beneficial owners of an account as well as their ownership percentages. While this requirement applies to retail accounts as well, beneficial ownership of corporate accounts can be significantly more complex.
  - Ownership of corporations frequently includes other corporations. This means that the beneficial owners of these entities, and their ownership shares, must also be identified. Complex corporate ownership structures can present significant challenges in tracing back to the ultimate beneficial owners and assessing the risk inherent in these ownership structures.
  - Corporations that are wholly or partly owned by overseas entities pose challenges in sourcing the data necessary to establish or verify beneficial

owners. Many overseas markets lack comprehensive business information databases such as Dun & Bradstreet or Moody's in the US and Bureau Van Dijk in Europe. Some business information for markets that use non-Latin scripts, such as China, Japan, and Russia, may only be available in those scripts.

These and other requirements result in significantly longer onboarding times for corporate and institutional clients. KYC and onboarding processes can vary from a few days for small and medium-sized enterprises (SMEs) to weeks or months for larger corporate clients in banking as well as institutional clients in the capital markets context.

MODERN KYC-CDD PARADIGMS

As know your customer requirements become more complex, financial institutions are supporting increasingly sophisticated processes that require more time, effort, and resources.

Entity Resolution and Holistic AML

A primary goal in KYC is achieving a holistic, 360-degree view of clients across the enterprise. This requires resolving a customer's relationship across multiple accounts, products, lines of business, and in some cases regions into a consolidated profile to obtain a fuller, more accurate picture of the customer's risk. Moreover, failure to capture comprehensive customer profiles exposes financial institutions to risk of financial crime schemes that may involve manipulation of multiple account relationships.

Compiling holistic customer profiles is typically a time-consuming task for analysts involving manual searches of internal customer and account data. Moreover, line of business, core system, and data silos act as a barrier to coordinating a single view of customers across the enterprise.

Risk Assessment

In addition to a holistic view of the customer's accounts, financial institutions need to understand interrelationships between customers and between accounts. Link analysis tools are often used to generate network maps of connections between customers, accounts, and transactional activity. Nevertheless, interpretation of link analysis visuals is still a labor-intensive due diligence task for the analyst.

A full approach to customer due diligence will also capture customers' relationships with parties outside the financial institution. This means capturing customers' external transaction counterparties and, as discussed earlier, beneficial owners. It also means searching external data sources, including public records as well as news and other media, to further understand the business and social context of the customer and, potentially, activities and affiliations that may indicate risk. This forensic process, essential to CDD and EDD, is also a highly manual, labor-intensive task for analysts and investigators.

Perpetual KYC

KYC-CDD is typically a one-time or at best periodic process lacking continuous client oversight, exposing financial institutions to risk due to client status changes. Increasingly, financial institutions are seeking to monitor client risk on a more regular basis, with some institutions seeing the need for perpetual monitoring for and alerting of risk indicators, such as an entity newly appearing on a watchlist or PEPs list.

Perpetual monitoring will ideally also involve dynamically linking KYC-CDD systems and behavior analysis systems. In this way, changes in customer risk due to screening hits or other KYC red flags would be passed to the transaction monitoring (TM) system. Conversely, alerts and other risk indicators from the TM system would be used to adjust customer risk profiles or trigger an EDD investigation into the flagged customer.

KYC in the Digital World

As consumer lifestyles and finances move to the online environment, requirements for KYC-CDD are intensifying. The fintech revolution, payments and other digital financial services, and online lifestyle services create demands for seamless, real time onboarding processes that do not adversely impact the customer experience or brand reputation.

Real time KYC processes used in digital services are often limited to simple screening checks. This potentially exposes the institution to customer risk. Exceptions and alerts may be handled by analyst teams, which are subject to the same challenges and limitations as for traditional financial institutions. Digital financial services need a more efficient, real time approach to KYC operations.

Shorter Corporate Onboarding Times

KYC processes in the corporate and institutional context are not only complex but also redundant, requiring corporate clients to provide their KYC information and documentation to each financial institution separately. Furthermore, as discussed above, corporate KYC processes often result in very long onboarding cycles. This creates significant inefficiencies for clients and financial institutions alike. The need for a more efficient approach led to the development of KYC “utilities” which serve as repositories for corporate KYC information that, once input by the corporate, can be accessed as needed by corporate banks or capital markets firms subscribing to the utility.

While KYC utilities have met with appreciable adoption, they are limited to both the corporates and financial institutions that participate in them. Taking a cue from the utilities, by supporting a self-service model whereby new corporate clients can provide their KYC information, financial institutions can optimize the corporate KYC process as well as offer a smoother onboarding experience for their customers.

APPLYING NEXT GENERATION TECHNOLOGIES TO KYC-CDD

Key Research Question 2

Which new technologies can support more efficient KYC-CDD processes?

Next generation technologies that are successfully supporting KYC-CDD include RPA and intelligent automation, unstructured data analysis, AI and machine learning, natural language generation, and cloud-based analytic tools.

Increased speed and efficiency in KYC-CDD is sorely needed to reduce the operational burden of compliance and to support the faster pace of digital financial services. Just in time, next generation technologies like intelligent automation are streamlining resource-intensive KYC processes and bringing them into the digital age.

Smart Robotics and Intelligent Automation

Robotic process automation (RPA) applied to routine processes such as transferring data between applications can of itself improve efficiency by automating manual processes. More effectively, RPA can be coupled with artificial intelligence techniques to deliver smart robotics and intelligent automation. Intelligent automation can automate KYC-CDD tasks including:

- Aggregation of internal customer data to create holistic views of customers across accounts, including deduplication and reconciliation of data in multiple back-end systems to aid in entity resolution.
- Collection and assembly of information from the relevant external data sources to construct entity profiles.
- Enrichment of alerts and cases using internal and external data.
- Creation of “dossiers,” in case management systems, that contain correlated KYC checks, alerts, and profile information and enrichments such as geolocation data.
- Analysis and presentation of beneficial ownership structures utilizing inputs from external business information databases.

Unstructured Data Analysis and External Data

The war for more effective KYC is to a large extent being fought on the battleground of unstructured data. In order to implement a risk-based approach to know your customer, financial institutions increasingly seek to understand the customer’s professional, institutional, political, and social context by searching large amounts of external data including news and media, public records, and other open-source intelligence (OSINT) data.

Traditional name search can find matches in external data but cannot provide the context in which the name appears, discern relationships with PEPs or high risk entities, or assess other risk indicators appearing in the sources. Natural language processing (NLP) and artificial intelligence techniques are needed to parse unstructured data and make these connections.

Crucially, advanced unstructured data analysis not only increases efficiency by automating labor intensive CDD processes, it can also identify relationships and risks that might otherwise go undetected.

AI and Machine Learning to Reduce False Positives

False positive alerts are the single biggest factor behind the massive expansion of AML-KYC operations at especially large financial institutions. Incumbent screening systems approach the problem with algorithms, token libraries, and known-customer lists, but with false positive rates often above 90% these methods clearly have their limits.

Advanced analytic techniques are being successfully applied to false positives reduction. Semantic analysis can help identify matches triggered by extraneous data, such as a word in the address rather than the entity name. Statistical analysis of customer information files can help identify high risk entities that may indicate a true positive. Results from analyst decisions can be fed back into the system to drive machine learning enabled prioritization algorithms to suppress likely false positives in the next screening run.

Some of the largest efficiency gains enabled by next generation technology have been in the area of false positives reduction. Various data collected by Celent suggest that these techniques have led to reduction in false positives of 30% to 70% or higher and 25% to 40% improvements in investigation efficiency.

Natural Language Generation

Advanced technologies can also increase efficiency in the regulatory reporting process, an arduous pain point in the AML-KYC value chain. RPA can be used to populate regulatory report formats with existing data and to electronically file the reports. Automated population of regulatory reports, however, has long been a feature of traditional AML-KYC reporting modules. The sticking point has been the suspicious activity report (SAR) narrative written by analysts.

Advancements in natural language generation (NLG) now enable the assembly of relevant case information into a coherent narrative to be provided to the analyst for review and emendation, thus supporting assisted report authoring.

APIs for Real Time Connectivity

The fintech and regtech revolutions have created an extensive ecosystem of service and solution providers relevant to AML-KYC. APIs are a crucial building block of this ecosystem that enable seamless connectivity to third-party providers such as data services and support real time KYC for payments transactions, digital financial services, and consumer lifestyle services.

Cloud-Based Analytics

Cloud environments can provide access to on-demand, high performance computing, virtually unlimited data storage, and advanced analytic tools including support for AI. Cloud-based solutions can provide organizations with advanced capabilities without the need to implement an in-house analytic platform or develop extensive internal data science resources.

As with other software as a service (SaaS) applications, cloud-based analytics solutions also relieve organizations of the need to maintain and upgrade software. Through continuous version releases, SaaS-based analytics can also provide accelerated access to advancements in technology.

CHALLENGES TO NEXT GENERATION KYC-CDD

While AI and other next generation technologies have shown success in improving efficiency and accuracy in KYC-CDD processes, various technical, operational, regulatory, and institutional challenges act as barriers to adoption.

Data Management and Integration

Data quality and data management have always presented challenges for AML-KYC operations. Data management continues to be a challenge in implementing next generation solutions.

- Data silos and redundant back-end systems inhibit the creation of holistic customer profiles, making integration, cleansing, and deduplication of data from multiple line of business systems a prerequisite for achieving a 360-degree view of customers.

- Data quality and gaps in data present challenges to entity resolution as well as risk assessment of customers.

- Sourcing specific types of data, such as beneficial ownership data or international KYC and business information, presents a further challenge, and specialized data providers have emerged to address some of these issues.

- From a regulatory perspective, GDPR and other data privacy regulation potentially limits the use of personal data such as social data for KYC purposes. At a minimum, such regulation requires the adoption of a data lineage framework for AML-KYC.

Computing Power and Capabilities

Next generation technologies may require significant processing and data storage capabilities. In the KYC-CDD context, this is particularly true of unstructured data analysis, which may involve processing large volumes of external data.

Development of proprietary, on-premise solutions incorporating AI, machine learning, RPA, or NLG require sophisticated technology and data science capabilities that are typically out of reach for any but the largest organizations. This reality is a major reason for the rapid emergence of regtech solutions that leverage next-gen tech for AML-KYC.

Regulatory Reliance on Rules

AML-KYC technology is dominated by a rules-based approach that has been developed over several decades with significant investment by financial institutions, software providers, and regulators alike. This has resulted in model governance programs — required by regulators — for rules development, refinement, and maintenance.

The regulatory emphasis on model governance and demonstrable results poses fundamental challenges to AI approaches to AML transaction monitoring and may also present a barrier to adoption of AI-based risk assessment and scoring in the KYC context.

Investment in Incumbent Technology

Organizations have invested heavily in their AML-KYC systems, operations, and organizations. This makes it harder to establish a business case for systems replacement or to implement the operational and resource changes needed to support a new technology paradigm. Regtech startups are responding to this situation by developing point solutions that may be layered on top of incumbent AML-KYC software. Incumbent

AML software providers, for their part, are developing machine learning, RPA and other next generation tools to supplement their existing solutions.

Institutional Resistance

Financial institutions are traditionally often risk averse, and this may be especially true of compliance departments. There are valid reasons to be concerned about entrusting sensitive customer and KYC data to cloud-based services or to be mindful of the need for new technologies to pass regulatory examination. As security and data issues for cloud services are addressed, successful case studies accumulate, and regulators become increasingly comfortable with AI, financial institutions will increasingly see next generation approaches to AML-KYC as a viable, if not the only, alternative to improving efficiency in AML operations.

Maturity of Technology

The application of AI, machine learning, robotics, and NLP to AML-KYC is still in early days. While these technologies have already demonstrated the ability to realize significant gains in efficiency and productivity, there are still limits to what they can achieve. Firms exploring the use of new technologies for KYC-CDD will have to determine whether their specific requirements can be met by conducting proofs of concept (POCs).

PROGRESS TOWARD NEXT GENERATION KYC-CDD

Key Research Question 3

What factors are supporting the adoption of next generation KYC-CDD technology?

Regtech focus on AML-KYC, AI initiatives by incumbent AML software providers, a growing track record of successful POCs and implementations, and regulatory initiatives supporting the use of next-gen technology for AML compliance are supporting progress in KYC-CDD technology.

While there are a number of challenges to the use of AI and other advanced technologies in the AML-KYC context, the case for next generation KYC is building. Factors supporting progress in KYC technology include:

Regtech Spotlight on KYC-CDD

AML-KYC is a primary focus of regtech, with some 25% of regtech firms working on this area. There is a similarly rich ecosystem of new tech firms working on identification and authentication, particularly for online services that require real-time authentication. Technology advancements have made instant authentication a reality for online marketplaces, e-commerce and digital lifestyle services.

More highly regulated sectors such as financial services still rely heavily on manual processes, particularly in investigating the many false positive alerts generated by legacy software. In financial services, the emphasis now is on increasing the efficiency and accuracy of these due diligence processes by means of AI / machine learning, robotics, and natural language generation. As discussed in the previous section, both regtech startups and incumbent software providers are introducing solutions.

Promising Track Record

Financial institutions have actively explored the use of AI for AML-KYC. Building on a number of successful POCs with their selected vendors as well as internal initiatives over the past several years, firms are now putting solutions into live production. While this activity has been concentrated among large institutions, the increasing availability of vendor solutions as well as the growing track record of next-gen AML technology is encouraging other firms to explore the use of these new approaches.

Growing Acceptance by Regulators

Jurisdictions ranging from the UK to Singapore are seeing the potential of AI to increase operational efficiencies, improve accuracy and mitigate risk, and (incidentally) significantly reduce the AML compliance burden. Regulators have initiated AML hackathons, like the UK Financial Conduct Authority's Global AML and Financial Crime TechSprint. Regulators in Singapore and the state of Arizona, among others, have implemented fintech and regtech sandboxes which have included AML solutions.

In the US, a remarkable joint statement recently issued by regulators including FinCEN, the OCC, and the FRB instructing banks to consider innovative approaches to "replace or augment existing BSA/AML processes" signals the inevitability of AI adoption in AML-KYC.

CONCLUSION — THE AI FUTURE OF KYC-CDD

Evolution in AML technology and the development of modern KYC operations, far from reducing the complexity of KYC processes, has resulted in ever evolving challenges and an increase in the operational burden of KYC compliance. The clearest demonstration of this paradox is the way in which more sophisticated, high volume techniques for matching entities against watchlists and ever-larger datasets has resulted in the ability to generate many alerts, but the majority of which are false positives. Advanced technology is needed to overcome this trade-off between alerts and false positives.

The use of next generation technologies for KYC-CDD has shown significant progress in answering this need. Intelligent automation and other next generation techniques are being used to create efficiencies by closing obvious false positives, delivering ready-made dossiers to analysts for investigation, supporting regulatory reporting, and other focused tasks.

This begs the question of how far technology can go in automating AML-KYC operations. Even though the use of AI and other next-gen tech in the AML context is a very recent development, we can already point to demonstrated successes across the AML value chain. Next generation AML technology is evolving rapidly and perhaps nowhere as quickly as in the KYC-CDD area.

Given this, it would seem to be not a question of if but of when technology will be capable of supporting fully automated AML-KYC processes. From a purely operational point of view, 100% automated KYC-CDD may be possible within a decade. The issue to be considered at that point will be whether AI-based KYC can render decisions as accurately as human analysts. This of will of course depend on whether (and when) truly cognitive computing can be achieved.

Fortunately, there is no need to wait for technology — or regulatory standards — to evolve to that point. The efficiencies achievable today within the context of analyst-driven AML operations means that the AI future of KYC-CDD starts now.

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 anti-money laundering and know your customer operations 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. 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

Accelerating AI Adoption in AML: New Solutions Opening New Horizons
April 2019

Deal Trends in the Anti-Money Laundering Systems Market
April 2019

AML Solutions for Smaller Financial Institutions: 2019 ABCD Vendor View
January 2019

Solutions for Watchlist Screening: 2018 ABCD Vendor View
November 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

Solutions for Anti-Money Laundering: 2018 Transaction Monitoring ABCD Vendor View
September 2018

Dawn of a New Era in AML Technology
September 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

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

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

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

Copyright © 2019 Celent, a division of Oliver Wyman, Inc., which is a wholly owned subsidiary of Marsh & McLennan Companies [NYSE: MMC]. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner. This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

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

Neil Katkov nkatkov@celent.com

AMERICAS

USA

99 High Street, 32nd Floor
Boston, MA 02110-2320

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

Rua Arquiteto Olavo Redig
de Campos, 105
Edifício EZ Tower – Torre B –
26° Andar
São Paulo SP 04711-904

Tel.: +55 11 3878 2000

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

Hong Kong

Unit 04, 9th Floor
Central Plaza
19 Harbour Road, Wanchai

Tel.: +852 2301 7500