CELENT

CSI

ACHIEVING HOLISTIC AML

FOCUS ON WATCHLIST SCREENING

Neil Katkov, PhD

CONTENTS

Introduction: Holistic AML compliance 1
Barriers to holistic AML 2
Establishing a centralized customer risk profile 4
Real-time screening to enhance AML compliance and deliver value to the business 6
Overcoming the AML - Anti-fraud divide through holistic solutions 8
Tackling false positives and supporting dynamic risk profiling with machine learning 9
Conclusion: Reducing risk through holistic AML compliance 10
Background 12
Leveraging Celent's Expertise 13
  Support for Financial Institutions 13
  Support for Vendors 13
Related Celent Research 14

INTRODUCTION: HOLISTIC AML COMPLIANCE

Now, more than ever, achieving a full, 360-degree view of customers is essential for optimized and effective anti-money laundering (AML) compliance.

Financial institutions — including banks, investment firms, and insurers — and the services they offer both retail and corporate customers have grown in size and complexity in terms of lines of business (LoBs), products offered, delivery channels including online and mobile, and regional and global footprints.

In addition, the rapid expansion of e-commerce, digital lifestyle services, and other online services is driving growth in online and in-app transactions and other new modes of transferring funds, introducing an entirely new realm of financial activity.

At the same time, in response to stricter regulation and more effective AML programs at financial firms, money laundering techniques have grown in sophistication in order to elude detection.

The complexity and reach of modern-day financial services provides the perfect terrain for money laundering schemes that use any combination of multiple customers, accounts, products, financial firms, and regions. The rapidly expanding ecosystems of e-commerce and online financial services provide even more opportunity for moving and cleansing illicit money.

To avoid being the unwitting host of schemes involving tainted funds, financial institutions and online services alike must be able to follow the money by tracking customer and account activity across the enterprise. They must also be able to assess the overall risk posed by customers holding multiple accounts as well as the risk inherent in networks of linked customers and accounts.

Holistic AML compliance, then, should capture a consolidated and coordinated view of customers and activity across lines of business, products, and regions — including state and, for multinational institutions, national borders.

Ideally, this would involve enterprise-wide capabilities in know your customer (KYC), watchlist screening, transaction monitoring, forensics, and case management operations. Furthermore, the rise of e-commerce, fintech and same day payments mean that these capabilities will increasingly need to be executed in real time or near-real time.

Unfortunately, data (of customers, accounts, and transactions), AML technology, and compliance operations are to a large extent still siloed in today's financial institutions. This fragmented environment is a very real barrier to achieving holistic AML compliance on an enterprise-wide level.

Many organizations are aware of this situation, yet still face a number of challenges in pursuing a holistic approach to AML compliance. Despite the barriers, by combining best-practice methodologies with appropriate technology, firms can achieve a sound framework for enterprise-wide compliance.

BARRIERS TO HOLISTIC AML

The benefits of a holistic approach to AML are clear. However, a number of barriers and challenges at organizations stand in the way of achieving a timely, enterprise-wide, 360-degree view of customers. Some of these barriers are:

- **Business, technology, and operational silos.** AML compliance at financial firms often follows the contours of the business, meaning that AML systems and analyst teams are siloed within the firm's various lines of business. It is not unusual for a bank, for example, to run separate AML compliance stacks for retail banking, corporate banking, capital markets operations, and wealth management.
  - For multinational firms, separate systems and teams are required for international operations, often on a country-by-country or at best regional basis, adding further complexity and opacity to AML compliance.
- **Disparate back-end systems and data**. Business and regional siloes beget system complexity in the form of multiple back-end systems and databases. In addition to transactional data, customer information is also often segregated according to line of business and product, preventing the firm from achieving a coordinated view of customers across the enterprise.
  - Historical accretion of core systems to support additional products and legacy systems introduced through mergers and acquisitions adds to system redundancy. For these reasons, it is not unusual for even a mid-sized financial firm to be running dozens of back-end systems; at large firms these may number in the hundreds.
- **The AML - fraud divide**. Both regulators and practitioners increasingly see AML and anti-fraud as complementary domains. On the technology side, software solutions that offer both AML and anti-fraud capabilities have long been available. Nevertheless, AML and anti-fraud remain separate areas of operation at most organizations. This creates yet more redundancy in systems and operations, and a further barrier to gaining a holistic, 360-degree view of customers and their activity.
- **Scalability of incumbent AML systems**. Financial institutions relying on legacy AML systems implemented years ago are likely to find these systems do not have sufficient scale to support AML screening and monitoring across the various lines of business, products, and operating regions; nor the capacity to support the numbers of concurrent analyst users needed to run a coordinated, enterprise-wide AML operation.
  - The large and growing data sets used in modern screening operations are another challenge. Screening systems in a best-practice compliance operation must be able to process multiple official watchlists, commercial entity databases and PEPs lists, various public databases, adverse news, and social data. Incumbent systems may lack both the scalability and the analytic capability to meet these big data requirements.
- **Lack of real-time capabilities**. While most legacy AML systems operate in batch mode, AML compliance increasingly calls for real-time screening, analysis, and decisioning. Sanctions screening for international wires was the first area to require real-time processing. AML and KYC compliance for e-commerce and online financial services also have real-time requirements. The move to faster payment types such as Same Day ACH is driving a parallel need for faster AML/KYC supported by real-time AML systems.

- **Resistance to AML replacement projects**. Newer technology with greater scalability, more sophisticated analytics, and real-time processing is available to overcome the limitations of legacy AML systems. Many organizations, though, may not have the appetite to undergo a full refresh of their technology. Rip-and-replace AML projects can be lengthy, disruptive, risky, and costly. Similarly, standardizing on one enterprise-wide AML platform remains an elusive goal for most firms, due to varying requirements among LoBs, the significant data management effort needed to achieve an enterprise-wide platform, and other factors.
- **AML Lite**. The cognate challenge at smaller financial institutions is achieving best-practice AML compliance with limited budgets and IT resources and on a more basic infrastructure. Smaller FIs need sophisticated, mature solutions in an affordable, manageable package.

Given the above barriers to meeting the evolving requirements of AML compliance, financial firms are increasingly challenged to find workable solutions to achieve timely, holistic AML and KYC compliance.

ESTABLISHING A CENTRALIZED CUSTOMER RISK PROFILE

Even for financial institutions facing challenges with their AML technology and operations, there are measures that can be taken to facilitate an enterprise-wide, holistic approach to AML and KYC.

One key is to establish a complete view of customer accounts and activity across the enterprise. Typically, financial firms maintaining multiple lines of business and operating across regions and geographies will, naturally enough, hold customer and account information from each operating division, and often each product, in separate databases.

The first step to achieving an enterprise-wide view of customers, then, is to consolidate this fragmented data to obtain a complete record of a customer's accounts across lines of business, geographies, and products.

To some extent, financial firms may have achieved this on the business side. For example, banks with relationship pricing programs or that offer their customers linked accounts, unified statements and other similar services will have multiple accounts rolled up under a single customer profile.

Building an enterprise-wide view of customers for compliance purposes involves a corresponding data management exercise for consumption by KYC and AML systems. Additionally, though, forensic analysis of customer attributes may be required to locate all relevant accounts. Customers may hold multiple accounts with inconsistent or varying identifiers for legitimate reasons, such as marriage or relocation. Money launderers, though, will purposefully endeavour to obfuscate their identity or relationships between accounts. Technology can help automate the task of uncovering such hidden linkages.

Customers licit and illicit may also establish accounts not only at multiple branches of an institution, but also across regions or countries. Truly enterprise-wide compliance would also capture these account relationships. Screening customers at international branches additionally may call for multilinguistic screening capabilities, potentially involving non-Latin scripts such as Arabic, Chinese, and Cyrillic.

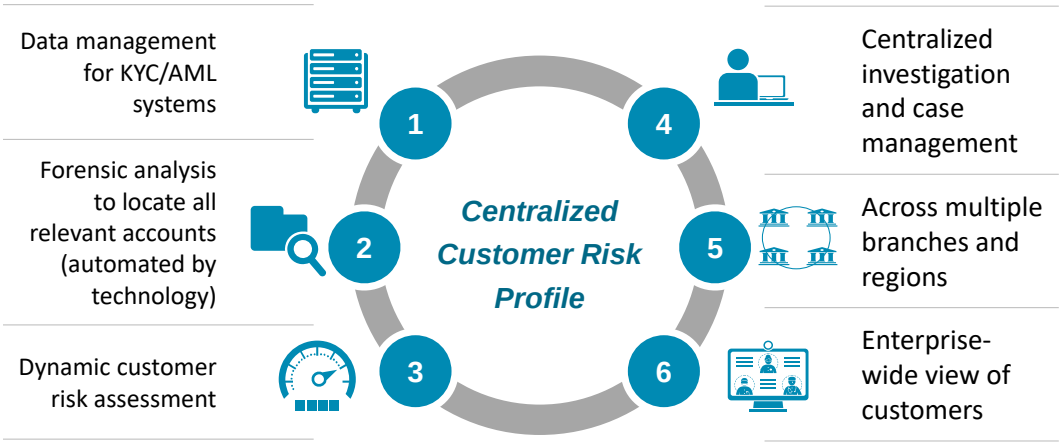
Crucially, holistic, enterprise-wide AML/KYC should also build a dynamic view of customer risk as it changes over time. Dynamic risk assessment involves capturing additional attributes on an ongoing basis, including:

- Updating customer risk profiles in an ongoing manner by incorporating risk factors/scores due to alerts from watchlist screening or transactional activity.
- Inputs from front office teams concerning risky customers or suspicious activity.
- Investigations, decisions, and filings by AML compliance analysts.
- Results of periodic customer review and rescreening of customers.

The final link in holistic AML is putting investigation of suspicious entities and behaviour on an enterprise-wide footing. Given the disparate, multiple back-end systems, data sources, and AML tools at many financial firms, this is often best achieved through a centralized investigation and case management capability.

Again, this can be achieved without wholesale replacement of systems, or standardization on one AML platform, by feeding outputs from multiple AML systems into a centralized case management tool for investigation of alerts and working of cases from throughout the enterprise, including the various lines of business as well as across regions/countries. Similarly, a central compliance dashboard can provide management with a coordinated view of AML risk across the enterprise.

Figure 1: Establishing a Centralized Customer Risk Profile



Source: Celent

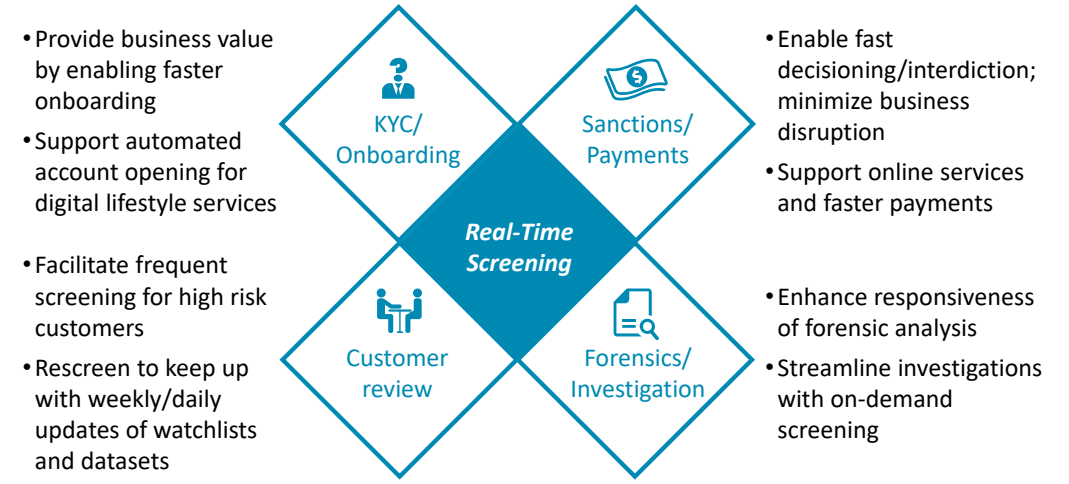
In this manner, a holistic, enterprise-wide, and dynamic view of customer risk can be achieved through:

- Creation of a consolidated view of customer relationships through data management and forensics, which supports…
- Screening and monitoring of these customer relationships on an enterprise-wide basis, which informs…
- Ongoing, dynamic assessment of customer risk profiles, and feeds into…
- Centralized case management and compliance dashboard systems for investigation of alerts and cases and assessment of risk on an enterprise-wide basis.

REAL-TIME SCREENING TO ENHANCE AML COMPLIANCE AND DELIVER VALUE TO THE BUSINESS

Traditionally, AML compliance has relied on after-the-fact batch processing. This is because of the focus on AML as an investigative process driven primarily by regulation. In this, it has differed from anti-fraud operations, which often leverage real-time processing and automated analysis in an all-out effort to stop fraud as it occurs and thus prevent bottom-line losses to the business.

Figure 2: Benefits of Real-Time Screening



Source: Celent

Increasingly, though, organizations are recognizing that real-time AML can not only enhance compliance processes, but deliver value-added benefits to the business as well. Use cases for real-time capabilities in the area of watchlist screening include:

- **KYC and Onboarding**. Simply put, real-time KYC checks provide business value by enabling faster onboarding, benefitting both the institution and their clients by facilitating streamlined account opening. Real-time single-name ID verification has long been in use by front office staff for account-opening purposes (as well as checks to support front office transactions). With the increasing emphasis on robust onboarding checks, going beyond ID verification to enable full-on KYC checks at the front office is becoming a best-practice requirement in onboarding.
  - Real-time KYC screening is also needed to support the seamless, automated account-opening processes required for e-commerce and online financial services, including the new generation of digital lifestyle services. In fact, digital services have become so prevalent that this sector has become a major driver of innovation in AML/KYC operations.

- **Sanctions and payments screening**. Sanctions screening of international wires is one of the most critical areas of AML compliance, as can be seen from the significant fines levied by regulators for noncompliance — reaching billions of dollars in several high-profile cases. Sanctions is also the compliance process most dependent on real-time capabilities, in order to enable fast decisioning and interdiction and to minimize business disruption resulting from delays in wires processing.
  - The need for real-time payments screening is expanding, driven not only by e-commerce, online financial services, and digital lifestyle services, but also by the move towards faster payments, such as Same Day ACH.
- **Rescreening for customer review**. Organizations need to keep abreast of the risk profiles of their customers, and for this purpose undertake periodic customer review by rescreening their customers against watchlists. While low risk customers may be reviewed monthly or quarterly, high risk customers require closer monitoring and hence more frequent screening.
  - Moreover, official watchlists and commercial entity databases are updated weekly and daily. Daily screening is becoming a best practice methodology in order to achieve dynamic and up-to-date risk assessments of customers. In this way, continuous due diligence is another important driver for real-time screening.
- **Forensics and investigation**. Despite gains in achieving real-time capabilities in various aspects of AML operations, alert investigation and forensics remain a heavily manual back-office function. Analyst operations are the primary driver in the rapidly escalating AML compliance costs at financial institutions. As a result, the search for more efficient processes to rein in costs is becoming a primary concern.
  - In this context, real-time, on-demand screening — especially when combined with automation support such as machine learning — can be an important tool in speeding up and streamlining investigations.

OVERCOMING THE AML - ANTI-FRAUD DIVIDE THROUGH HOLISTIC SOLUTIONS

Anti-fraud and anti-money laundering operations have much in common. Anti-fraud also relies on screening to identify customers and check them against fraud lists; and on transaction monitoring to detect patterns of activity that might suggest fraud. Moreover, regulators increasingly see anti-fraud operations as under their purview, due to ties between fraud and money laundering activities, and as an area of organized financial crime in its own right.

Nevertheless, anti-fraud and AML operations continue as separate at most organizations. This is likely to change, however, as the technology tool kit used for each of these areas converges. AML compliance is making greater use of techniques long used in anti-fraud, such as real-time capabilities, advanced analytics, and automated workflow. Greater regulatory oversight over fraud may also lead firms to take a more coordinated approach to anti-fraud and AML.

Implementing an enterprise-wide alert investigation and case management capability that encompasses both AML and anti-fraud is an effective first step in this journey. In this way, holistic AML and anti-fraud investigation can be achieved without replacing or disrupting existing screening and behaviour detection systems. Case management and control-and-command solutions can integrate feeds from AML and anti-fraud systems to provide consolidated investigation and analysis across these domains.

From a technology and operations perspective, coordinating AML and anti-fraud has obvious potential for efficiency gains. Yet its greatest value lies in enabling integrated analysis of suspicious customers and transaction patterns across money laundering and fraud scenarios. This can be a powerful tool to uncovering entities and activity that might otherwise go undetected. A holistic AML and anti-fraud program is also further indication to regulators that the institution is taking a strategic approach to combating financial crime.

TACKLING FALSE POSITIVES AND SUPPORTING DYNAMIC RISK PROFILING WITH MACHINE LEARNING

AML compliance costs have soared over the past decade, with spending growing in the double digits at many financial institutions. While the ultimate cause is a continued increase in regulations and regulatory oversight, much of this pressure has become manifest in a single, searing pain point: false positives, or alerts that upon investigation prove to be innocent entities or transactions.

At many firms, screening and monitoring technology — together with the rules, parameters, and tunings used to configure them — generate high percentages of false positives. False positive rates over 20% are common; rates over 70% are not unheard of. This means that too many entities or transactions are being flagged by AML and KYC systems. It falls to AML compliance teams to investigate these alerts through largely manual processes.

The expanding operational burden created by false positives is not sustainable for financial institutions. Fortunately, a new generation of technologies including machine learning is emerging that can help increase efficiencies in the AML compliance process.

Essentially, machine learning refers to adaptive computing techniques that use the outcome of tasks as inputs into the next iterative run, so that the software produces better results each time it performs the task. In the AML screening context, machine learning can be used to progressively incorporate decisions on alerts made by analysts as well as by the system itself, so as to more efficiently process future alerts.

Machine learning can be used to segment screening hits into high priority alerts that are likely to point to true suspicious entities and low risk alerts that can be deemed false positives. By automating triage of alerts in this way, machine learning can significantly reduce the workload performed by analysts. This introduces much-needed efficiencies into AML compliance operations and allows analysts to spend more time on high-priority investigation.

Implementing machine learning as part of an enterprise-wide, holistic AML program can help maximize the learning effect by leveraging inputs from multiple lines of business throughout the organization.

By bringing an automated, iterative approach to the process of weeding out false positives, machine learning can make it easier for firms to make frequent screening a part of their AML program. By associating data from throughout the enterprise to facilitate accurate risk assessment, machine learning can help support dynamic, continuous risk profiling.

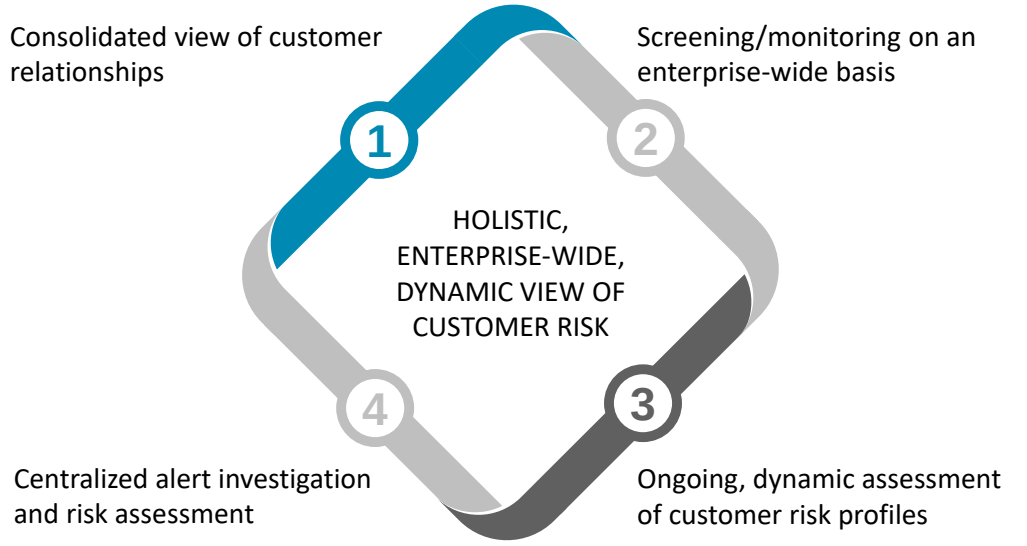
CONCLUSION: REDUCING RISK THROUGH HOLISTIC AML COMPLIANCE

Financial services firms including banks, investment firms, and insurers today operate in a complex environment involving multiple lines of business; new digital channels along with traditional branch and agency operations; and extensive regional or global footprints. Moreover, e-commerce, digital lifestyle services, and other online services are introducing new modes of online and in-app transactions.

The broad scope of these operations makes an enterprise-wide, holistic approach to AML of central importance in order to minimize vulnerabilities and reduce regulatory and reputational risk.

At many firms, though, AML technology and operations are decentralized and organized by line of business or geography. This siloed approach to compliance is a serious barrier to achieving a holistic, 360-degree view of the customer for risk assessment purposes. At the same time, most firms do not have the appetite for full scale rip-and-replace projects in order to build these needed enterprise-wide capabilities. Moreover, smaller financial institutions are challenged to implement sophisticated capabilities in an affordable and manageable way.

Figure 3: Model for Holistic AML



Source: Celent

Given such challenges, many firms are focusing on adding strategic components to their AML compliance stack in order to achieve enterprise-wide AML in an efficient manner. The following program components can help support a holistic approach to AML:

- A centralized approach to building customer risk profiles.
- Real-time screening to support faster onboarding, same day payments, and digital services.
- AML and anti-fraud programs integrated at the enterprise level.
- Advanced technologies such as machine learning to reduce false positives and support dynamic risk profiling.

Implementing enterprise-wide AML can be an effective way to overcome limitations of legacy compliance solutions, while at the same time supporting AML compliance operations in today's rapidly changing financial landscape.

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

BACKGROUND

This report was commissioned by CSI; however, the analysis and conclusions are Celent's alone, and CSI had no editorial control over report contents.

Computer Services, Inc. (CSI) delivers core processing, managed services, mobile and Internet solutions, payments processing, print and electronic distribution, treasury management, and regulatory compliance solutions to financial institutions and corporate customers across the nation. Exceptional service, dynamic solutions, and superior results are the foundation of CSI's reputation and have resulted in the company's inclusion in such top industry-wide rankings as the FinTech 100, Talkin' Cloud 100 and MSPmentor Top 501 Global Managed Service Providers List. CSI's stock is traded on OTCQX under the symbol CSVI.

For more information about CSI, visit www.csiweb.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 AML 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 [list several here]. 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

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

Innovation in Compliance Technology: Emerging Themes and Vendor Solutions
June 2017

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

Emerging Solutions in Anti-Money Laundering Technology
April 2015

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

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

Neil Katkov, PhD nkatkov@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 Cedex 16
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