COGNIZANT

Digital Customer Due Diligence: Leveraging Third-Party Utilities

With industry pressures and changing customer expectations, it has never been more important for financial services organizations to offer a fast and efficient client onboarding experience. By leveraging digital technologies, automation and third-party models, banks can successfully navigate the complexities of this process.

Executive Summary

Amid growing competition in the financial services industry, organizations are struggling like never before to balance regulatory requirements, operating expenses, customer expectations and new client acquisitions. In this scenario, the complex process of client onboarding has acquired top significance.

Banks must contend with a wide range of global regulations, including the Fourth EU Money Laundering Directive (4MLD), the Financial Crimes Enforcement Network's (FinCEN) Final Rule on Beneficial Ownership, the Dodd-Frank Act, the Foreign Account Tax Compliance Act (FATCA), the Fair and Effective Markets Review, the Markets in Financial Instruments Directive (MiFID II), BASEL III (the Basel Committee on Banking Supervision's regulation number 239), the Foreign Corrupt Practices Act (FCPA) and local implementations of anti-corruption and anti-bribery legislations.

Above all, compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements has posed the biggest challenge for banks and regulators alike. Since 2008, financial powerhouses have had to pay heavy penalties for noncompliance[1] (see Figure 1, next page).

In this paper, we explore emerging approaches to client onboarding that leverage digital technologies and third-party utility models. We also provide an overview of the utility service provider landscape and suggest a framework for selecting the best model and provider for client due diligence for institutional and corporate clients.

Client Due Diligence Challenges

The complexities, challenges and difficulties inherent to client onboarding include the following:

- **Data quality:** Banks face numerous challenges when collecting required data for client due diligence (CDD). Information received from the public domain is often inaccurate, and clients often have privacy concerns when it comes to sharing personal information. Bank employees are hesitant to pressure clients for fear of antagonizing them.

Cognizant

Penalties Imposed on Global Banks for AML/KYC Noncompliance

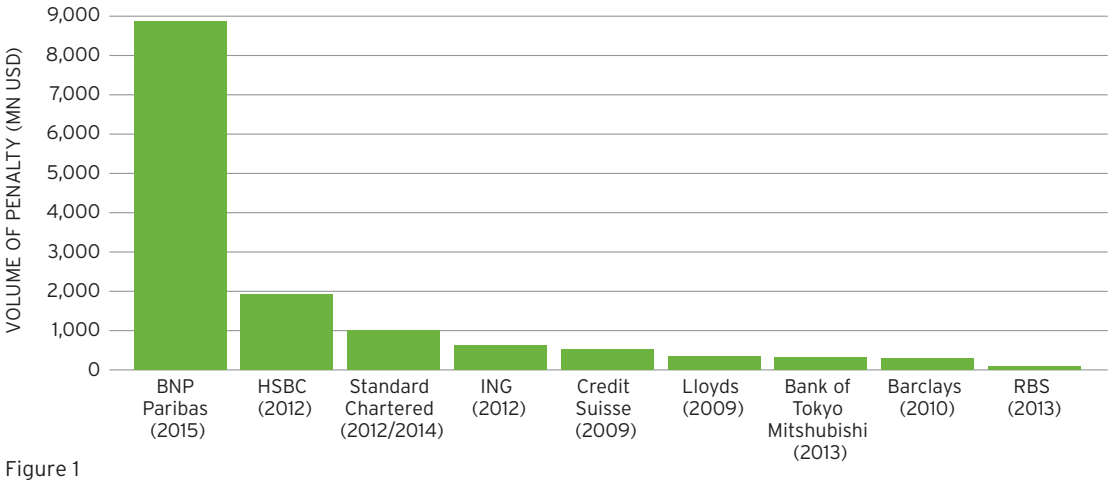

Figure 1
Source: Cognizant analysis of publically available data.

- **Ascertaining the ultimate beneficial owner (UBO):** This is perhaps the most daunting CDD requirement, particularly with the increased pressures of FinCEN's recently released Final Rule on Beneficial Ownership and the 4MLD regulation. Currently, the U.S. has not set regulatory restrictions for determining the UBO, but in the European Union, banks are required to identify individuals with 25% or more equity interest in a legal entity. Most banks lack a well-established policy to determine the UBO for new accounts.
- **Lengthy turnaround time:** The current CDD process is cumbersome and time-consuming, with bank employees relying heavily on complex spreadsheets and manual processes to assess AML risk for a client. The process is plagued by delays and manual workarounds.
- **Siloed processes and lack of standardization:** In the absence of a standardized AML risk assessment template, the processes and rules for collecting, maintaining and updating client data differ vastly across most banking organizations. Multiple siloed systems and user interfaces are used for client onboarding and maintaining client data. Different lines of business use different search tools, and document storage methods and locations are varied.
- **Ever-changing regulatory requirements:** Because global banks come under the purview of multiple regulatory bodies, their internal systems need to be agile enough to accommodate these varied and often contradictory requirements across geographies.

The Promise of Digital and Automation

The financial services industry is awakening to the value of automation and digitization in organizations' KYC and CDD processes and the promise of reduced costs and enhanced customer experience.

Regulators across geographies are increasingly willing to support banks' efforts to embrace digitization and automation. For example, the UK's Financial Conduct Authority, the Monetary Authority of Singapore and Bank Negara Malaysia have developed specific innovation agendas that include partnering with the wider financial services industry.

Some digital initiatives in which banks are currently investing include self-service digital channels for CDD, maintenance of client documents in a centrally managed repository, stringent role-specific access control mechanisms, and a rules engine with embedded logic to assess whether regulatory changes will impact clients.

Digitization can optimize the CDD and AML/KYC processes in the following ways:

- **Parallel processing of "new-to-bank" client onboarding,** aided by a rules-based workflow engine and automation of manual activities. This can substantially reduce turnaround time for account opening.
- **Mobile and web-based apps,** which can assist users with onboarding review tasks for their assigned client cases. Apps are also available to support e-signatures and reporting.

- **Form digitization,** which can substantially reduce processing time. The dynamic nature of these forms allows users to modify content online.

The most interesting aspect of digitization, however, is process automation. Client onboarding involves multiple sub-processes, such as data collection, KYC and AML, credit assessment, risk profiling, account setup, activation and internal reference data updating. Each sub-process is handled by a separate department. It becomes more complex when a client opens various banking relationships, such as an investment account and a line of credit, at different points in time. In the traditional CDD environment, different lines of business within the bank work in isolation, leading to duplicate client data collection. This is both aggravating for the customer and also time-consuming.

Banks are now trying to automate large parts of the process for low-risk clients. While this can result in substantial cost savings and operational improvements, automation requires a considerable upfront investment. Because CDD/KYC is not a differentiating function for banks, many are seeking a new operating model for these processes.

Shared Third-party Utility/Managed Services Model

Over the past two to three years, many market utilities for KYC, AML and customer reference data have emerged globally. These utilities facilitate smooth client onboarding and regulatory compliance by providing central repositories for KYC and AML data, as well as related documentation.

A third-party KYC utility maintains a central repository of client information and documents required for the bank's CDD procedure for client onboarding and subsequent monitoring. Once client data has been fed into the utility system, member banks can pay a fee to access the repository and leverage the information for their KYC and risk assessment functions.

Third parties can facilitate smooth client onboarding and regulatory compliance by providing central repositories for KYC and AML data, as well as related documentation.

There are three types of third-party KYC utilities:

- **Industry collaboration utility:** These utilities are formed from joint ventures between a third party and a specific bank; the provider develops a customized utility in collaboration with the bank.
- **Jurisdictional utility:** These organizations are based on a specific geographic jurisdiction (such as the European Securities and Markets Authority's European Market Infrastructure Regulation), and perform due diligence of all entities governed by that jurisdiction.
- **Utility service provider:** These providers create their own products and market them as a service to banks.

This paper primarily focuses on the third category.

Bank/Third-Party Utility Provider Operating Model

When a bank collaborates with a third-party utility provider, it first checks whether data on the newly acquired customer/prospect is available in the shared KYC utility database, and requests access from the customer. If the data is not available, the provider collects and stores the relevant data for the bank to access and store in its own database for future use.

Regulators lack a clear view on the accountability of third-party utilities and managed services providers. However, KYC utilities should never be considered as a substitute for banks' compliance responsibilities. They are merely facilitators responsible for collecting and collating end-user information and documents on behalf of banks. Banks remain solely responsible for customer risk assessment.

A bank may need to supplement the services provided by the KYC utility services provider in order to ascertain the suitability of a prospective client in accordance with its risk appetite and internal policies. Because of this, banks should seek a provider that uses consistent processes and can align itself with the bank's policies for more comprehensive coverage of the CDD processes and requirements. The provider should also be able to quickly adapt to regulatory change. Figure 2 (next page) illustrates the functions that are best outsourced to third-party vendors and those that should be retained in-house.

Accountability Matrix for Banks and Third-party Vendors

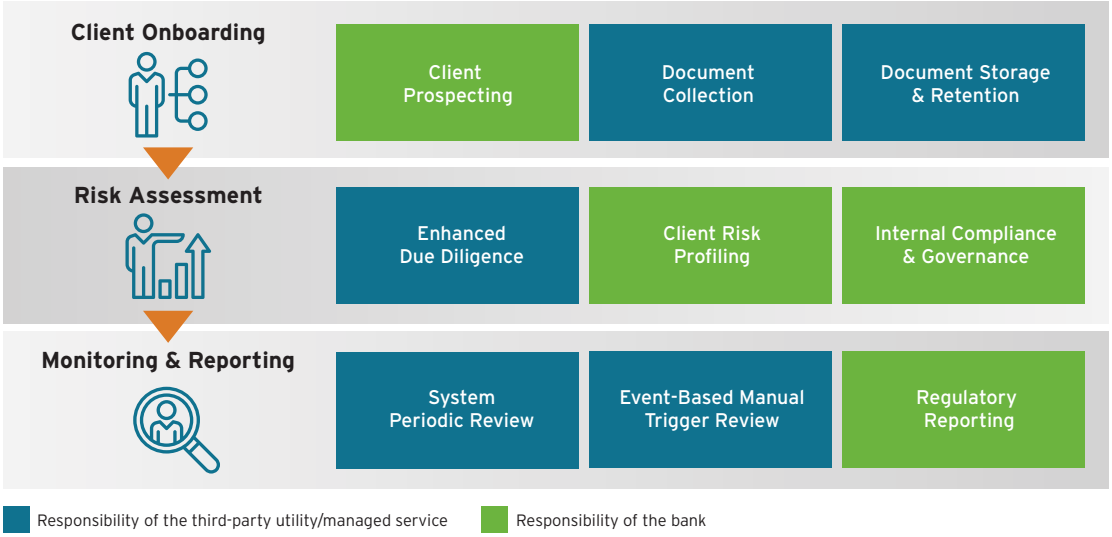

Figure 2

Managed Services Model

A managed services model goes beyond collecting, storing and distributing client data. In this model, the bank outsources a large portion of the CDD process to a third party, thereby reducing the overall cost of the entire process and increasing standardization. Third-party entities providing end-to-end CDD solutions have a dedicated team of KYC and AML experts who help collect and verify client information and documents, determine the UBO for the client, and screen end-clients and all relevant parties. This approach can be delivered as infrastructure as a service (IaaS), platform as a service (PaaS) or data as a service (DaaS).

Unlike a static utility, a managed service can help banks monitor client data in real time. In the current economic scenario, numerous events can drastically alter the perceived risk for a client. These include:

- Changes in executive management.
- Adverse events that lead to negative media coverage.
- Business expansion into new geographies.
- Addition of new lines of business.
- Taking the organization public.

The managed service proactively helps the bank monitor key changes in its client base that would otherwise be revealed only during periodic system reviews that occur annually or even less frequently, depending on the client's risk rating. When a client's status changes, documents expire, or critical information emerges, the dedicated KYC and AML team will alert the bank, which can then assess the situation and conduct an ad-hoc review of the client. This minimizes risk for the bank and decreases its exposure to prohibited entities and politically exposed persons (PEP).

Benefits of partnering with a managed service provider include:

- Substantial savings on manpower and asset costs.
- An error-free and robust KYC function.
- Assurance that the client data received is the most recent and has factored in various internal and external events.
- Scalability across geographies and LOBs seamlessly.
- Secure data storage.

Using a managed service benefits both the bank and its clients. For clients, managed services providers offer control and visibility over their own data and information. Clients can store, distribute and control access to their data in a secure environment, eliminating duplicate efforts to furnish information. Also, the client does not have to pay for these services.

Deciding Between a Utility Service and a Managed Service

Banks tend to choose a managed service provider to perform high-volume, less complex functions that are not critical in nature, such as periodic client reviews, client onboarding and adverse media coverage screening. The following are the typical characteristics of a managed service engagement.

- **The end-to-end workflow is managed in most cases by a vendor** (an IT service provider).
- **Initial setup cost is high,** as the required resources and infrastructure must be in place.
- **Contracts are usually multiyear programs** in order to extract benefit from the high initial cost.
- **Scalability is critical** to the success of a managed services contract.

A utility service is characterized by the following features:

- **It usually manages critical and complex processes,** such as transaction monitoring, suspicious activity reporting (SAR) and risk ascertainment.
- **Tasks are extremely sensitive** to the bank and are completely controlled internally.

Laying the Groundwork

There is no paucity of third-party utility services and managed services providers available today, and a host of players has mushroomed over the past few years. Broadly, there are six parameters that banks should consider when selecting a managed service or third-party utility provider (see Figure 3).

1. **Accountability for regulatory compliance:** Financial regulations are mostly regional in nature; hence, not only do the KYC and AML policies for a multinational bank vary across countries, but the bank must also tweak the risk assessment rules and guidelines for each geographic location. External service providers should be able to quickly comprehend and adapt to regulatory changes.
2. **Legal/data privacy requirements:** Banks need to consider the legal implications when selecting a utility provider. Data privacy laws in various countries do not allow data to be stored and maintained in other countries/jurisdictions. The bank should consult data privacy lawyers before entering into a contract with any utility provider.
3. **Impact on internal operations:** The bank needs to amend its systems so that when the third-party utility provider takes over, its approach to providing information and other inputs is aligned with existing KYC policies, activities and systems. The bank's objective is to transition as seamlessly as possible. The KYC utility/managed services provider might begin by providing information about clients, and gradually move toward delivering on its entire array of services.
4. **Governance capabilities:** The bank needs to have a proper governance structure in place. The quality of deliverables furnished by the utility/managed services provider should be evaluated regularly to ensure it meets expectations and the bank's organizational objectives.

Factors to Consider for Partner Selection

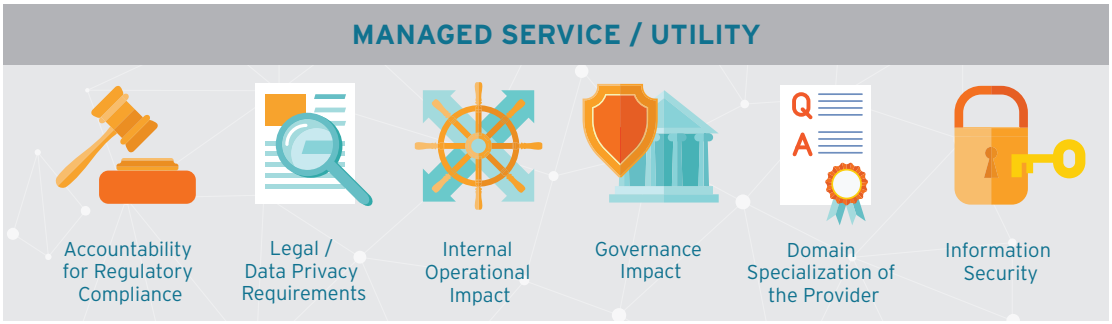

Figure 3

Quick Take

Choosing Between Domain Specialization and an Enterprise-Wide Solution

Banks need to assess which approach best meets their needs.

Advantages of best-of-breed solution providers include:

- **Cover a niche requirement:** If the bank has a specific requirement (e.g., a document maintenance suite), it can choose a niche product that can be easily plugged into the bank's existing system.
- **Faster roll-out:** Compared with an enterprise solution, these solutions take much less time to implement, as only a small part of the workflow is impacted.
- **Less expensive:** These solutions are less expensive than an enterprise-wide suite. However, if the bank needs more of these solutions for its other niche requirements, the overall cost would increase, with additional license and support fees.

Advantages of an enterprise-wide solution include:

- **Meets enterprise-wide requirements:** These solutions are ideal for banks seeking a comprehensive solution for their KYC workflow.
- **Easy to upgrade and scale:** Enterprise solutions have multiple features that can either be introduced from the outset or in stages when the bank needs them. These solutions allow the bank to turn off features that are not needed initially and then introduce them at a later stage through a simple admin setting. They also come with a robust user management tool that helps scale usage volumes and introduction of more users.
- **Integrated solution:** An enterprise solution is integrated, and as the solution grows and adds more functionality, complexity does not increase, which is very beneficial in the long run.

5. **Domain specialization:** Providers generally offer either an enterprise-wide solution or a niche domain/function-specific product (provided by "best of breed" solution providers). The choice depends entirely on the bank's requirements. (See Quick Take above for the pros and cons for each category.)
6. **Information security:** Given that sensitive customer information is at stake, the bank must consider the heightened risks in today's environment of data hacking and data theft. Financial institutions must be certain that the external service provider has a robust information security system and disaster recovery system and processes in place.

In addition to these requirements, factors such as the provider's reputation, its client base, financial soundness, implementation support and training and after-sales service should also influence the bank's choice of vendor.

Before choosing a third-party provider, the bank should conduct a pilot of services offered by the utility provider prior to the actual implementation, as well as develop proper operating guidelines, process flows, and a roles and responsibilities matrix. The financial institution should also establish a resilient internal governance model to manage the engagement with various KYC utilities. The features of a strong third-party utility product are detailed in Figure 4.

Attributes of an Ideal Third-party Utility

Tracking Attributes
- Suspicious activity tracking.
- UBO determination.
- Risk scoring based on multiple assessment parameters.
- Dynamic questionnaire based on client type (e.g., financial/non-financial).
- Configurable detection rules.
- Automated periodic screening of client to ascertain risk rating.

Workflow Attributes
- Consolidated case management tool.
- Built-in flexibility to modify workflow.
- Multi-user access on same case at various stages.
- Seamless data mapping for compliance reporting sought by multiple regulators across geographies.
- Real-time alert generation.

Data Attributes
- Adverse media report coverage across geography.
- Integration with various sanctions checklists.
- Integration with PEP checklists (OFAC).
- Integration with available public records across geographies.

Figure 4

Features of a Strong Third-party Utility Product

Banks should consider the following product suite-specific features:

- **Product feature sophistication and flexibility:** The most important attribute of a third-party service is its level of sophistication, and the embedded flexibility to adapt to changes in requirements. The system should have embedded features to seamlessly integrate the front-, middle- and back-office systems.
- **Breadth of functionality:** The solution should cover multiple lines of business and domain areas, and should be able to cater to regulatory requirements across geographies.
- **Computational power and analytics:** Key factors that banks should consider when assessing system robustness include the computing power of the screening and risk profiling system, its ability to handle bulk data and sudden surges in data load, and turnaround time for analyzing and presenting data.
- **User-friendly GUI:** The interface should be simple and user-friendly. Since users across lines of business and geographies will interact with the system, a refined and intuitive dashboard is a must.
- **Reporting capability:** This is one of the most critical and sought-after features. The product should be able to carry out timely analysis of the huge volume of data and present it to the end-user in the form of various reports. It should be able to handle ad-hoc requests and generate custom reports (e.g., requested by financial regulators) and dashboards.

Pricing Structure

Vendors offer a variety of pricing structures, including the following:

- **Flat annual fee:** Most third-party providers use a flat-fee structure for charging their clients. Under this structure, the bank must pay the annual fee regardless of the number of times it has used the provider's service during the year.
- **Hybrid fee:** The fee is a combination of a fixed and a variable component. The variable component depends on the type of service availed, the data volume to be processed, etc.
- **Pay-per-use fee:** Beyond a minimum annual amount, the fee is based on client usage.
- **No fee:** Such services are offered by the entities that provide the information (e.g., asset management companies, corporates).

Large global banks such as Citibank, HSBC Bank and Deutsche Bank will typically opt for the flat-fee structure because of the large number of clients they onboard and their high transaction volumes. Smaller banks (e.g., community banks or credit unions in the U.S.) that are concentrated within a country or region may choose a pay-per-use structure as they may onboard only a small number of clients each year. Medium-sized banks will likely opt for hybrid pricing. A super-regional bank (e.g., Key Bank or PNC Bank) would fall in this category.

The Road Ahead

Over the past few years, numerous third-party utility services have cropped up in the fintech space servicing the KYC/AML area for banks. As mentioned earlier, their offerings cover three areas:

- Solicit, collect and maintain end-client information and supporting documents for banks.
- Various screening and validation operations (PEP, sanctions, etc.).
- Ongoing monitoring, audit and reporting.

Third-party Players in the AML/KYC Space

THIRD-PARTY PROVIDER	PRODUCT/SUITE	FUNCTIONAL AREAS COVERED
Thomson Reuters Corp.	Org ID	CDD, KYC, SAR monitoring
NICE Systems / Actimize, Inc.	Actimize	SAR monitoring, CDD, FATCA compliance, watchlist filtering, currency transaction report (CTR) processing and automation
Fenergo	Fenergo Client Onboarding Module Fenergo Regulatory Compliance & Review Management Module Fenergo Regulatory Onboarding	CDD, client onboarding, ongoing client review, adverse media coverage, AML , KYC, client off-boarding
BAE Systems	NetReveal	AML, transaction monitoring, CDD, KYC, watchlist management, sanctions, PEP screening
HIS Markit	kyc.com	Client onboarding, CDD, KYC
Wolters Kluwer Financial Services	OneSumX Solutions	AML, CTR, CDD KYC, governance
Accuity FircoSoft (part of RELX Group)	Firco Continuity Firco Trust Global Watchlist Firco Compliance Link	Transaction monitoring, name screening, watchlist management, regulatory screening
Arachnys	Arachnys D3 Arachnys Investigator	CDD, PEP screening, adverse media coverage

Figure 5

Figure 5 lists some of the prominent providers operating in this space, the products/suites they offer and their functional areas of expertise.

We expect a moderate shakeup in the industry, followed by a consolidation over the next few years. A handful of players with a global presence will eventually dominate. Consolidation appears to have already begun with the acquisition by London-based RELX Group (which owns LexisNexis and Accuity) of French AML/KYC solution provider FircoSoft in September 2014.

This trend is expected to benefit both banks and providers. Banks will be able to choose from among a few providers, all of which possess strong credentials, while providers will be able to charge higher rates for their services given the reduced competition.

Regulators will need to play a more decisive role in the "bank-utility" model. They need to standardize requirements rather than leaving it to banks and providers. The KYC/AML processes adopted by third-party providers should also be meticulously scrutinized and audited.

As compliance and regulatory risks continue to grow with business expansion across geographies, banks must strive to stay ahead of the curve through early adoption of appropriate technologies and partnerships with third-party AML/KYC vendors. Such partnerships will help banks achieve the flexibility they need to scale their business and expand into new markets. In this way, banks can meet the ever-increasing expectations from their clients by boosting the efficiency and effectiveness of customer onboarding.

Footnotes

[1] Data obtained from the following sources:

David Benoit, "Standard Chartered's Fine Tally Runs to $667 Million," *The Wall Street Journal*, Dec. 10, 2012, http://blogs.wsj.com/deals/2012/12/10/standard-chartereds-fine-tally-runs-to-667-million/.

Reed Albergotti, "ING Fined a Record Amount," *The Wall Street Journal*, June 12, 2012, http://www.wsj.com/articles/SB10001424052702303901504577462512713336378.

Claudio Gatti and John Eligon, "Iranian Dealings Lead to a Fine for Credit Suisse," *The New York Times*, Dec. 15, 2009, http://www.nytimes.com/2009/12/16/business/16bank.html.

James Quinn and Katherine Griffiths, "Lloyds TSB Agrees to Pay Fine of $350M for Sanctions Help," *The Telegraph*, Jan. 10, 2009, http://www.telegraph.co.uk/finance/4213151/Lloyds-TSB-agrees-to-pay-fine-of-350m-for-sanctions-help.html.

Karen Freifeld, "Bank of Tokyo Mitsubishi to Pay $315 Million over Whitewashed Report," Reuters, Nov. 18, 2014, http://www.reuters.com/article/us-btmu-sanctions-settlement-idUSKCN0J21R320141118.

Andrew Clark, "Barclays Fined $298M for Sanction Breaking," *The Guardian*, Aug. 16, 2010, https://www.theguardian.com/business/2010/aug/16/barclays-fined-for-sanction-breaking.

Aruna Viswanatha and Anna Yukhananov "RBS to Pay $100 Million in U.S. Sanctions Probe," Reuters, Dec. 11, 2013, http://www.reuters.com/article/us-rbs-sanctions-idUSBRE9BA0Y120131211.

About the Author

Biswadeep Sengupta is a Consulting Manager within Cognizant Business Consulting's Banking and Financial Services practice. He has functioned as a lead business analyst and consultant for various bank implementation projects across the EU, North America and Asia-Pacific. Biswadeep's areas of expertise include asset and wealth management, retail banking, wholesale banking and consumer lending. He holds an MBA in finance and strategy and can be reached at Biswadeep.Sengupta@cognizant.com.

About Cognizant

Cognizant (NASDAQ: CTSH) is a leading provider of information technology, consulting, and business process services, dedicated to helping the world's leading companies build stronger businesses. Headquartered in Teaneck, New Jersey (U.S.), Cognizant combines a passion for client satisfaction, technology innovation, deep industry and business process expertise, and a global, collaborative workforce that embodies the future of work. With over 100 development and delivery centers worldwide and approximately 255,800 employees as of September 30, 2016, Cognizant is a member of the NASDAQ-100, the S&P 500, the Forbes Global 2000, and the Fortune 500 and is ranked among the top performing and fastest growing companies in the world. Visit us online at www.cognizant.com or follow us on Twitter: Cognizant.

Cognizant

World Headquarters
500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277
Email: inquiry@cognizant.com

European Headquarters
1 Kingdom Street
Paddington Central
London W2 6BD
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102
Email: infouk@cognizant.com

India Operations Headquarters
#5/535, Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060
Email: inquiryindia@cognizant.com

Codex 2386