dun & bradstreet

How Compliance Practices Should Adapt to Increased Beneficial Ownership Scrutiny

An Auditor's Recommendation to Build a Robust Beneficial Ownership Program

By Yunhong Liu, CAMS-Audit
Dun & Bradstreet

TABLE OF CONTENTS

ABOUT THE AUTHOR

Yunhong Liu,
CAMS-Audit, PMP

Sr. Director, Head of APAC Compliance Solutions
Global Compliance Solutions
Dun & Bradstreet

Hong is a compliance subject matter expert with extensive international experience and 10+ years background in Compliance, Data management and banking Operations. Hong covers AML and Anti-Bribery/Corruption practices for large global accounts.

Prior to joining D&B, Hong worked for BNP Paribas and Goldman Sachs where she managed client on-boarding(BSA/AML, KYC), client reference data governance, derivatives clearing and compliance projects and practices.

Hong holds a Bachelor's degree in International Finance and a Master's degree in Accounting as well as an MBA from CU Leeds School of Business. Hong is an Advanced Certified Anti-Money Laundry Specialist with focus on Compliance Audit (CAMS-Audit). The CAMS-Audit designation is an advanced-level certification and is the first of its kind in the AML and financial crime prevention community.

EXECUTIVE SUMMARY

Today effective Beneficial Ownership (BO) and Ultimate Beneficial Ownership (UBO) identification and verification have become an essential component of the client onboarding process. BO identification and verification is a requirement for financial institutions to meet Know Your Customer (KYC), Anti-Money Laundering (AML), tax, sanctions and Foreign Account Tax Compliance Act (FATCA) regulations as well as other compliance laws. Furthermore, scrutiny has been expanded to almost all industries, especially high risk sectors such as Real Estate and Casinos.

There are many challenges to implementing an effective BO program. Various regulations provide dissimilar BO definitions as well as threshold and due diligence requirements. Some regulation such as the Financial Crimes Enforcement Network (FinCEN) Notice of Proposed Rulemaking (NPR) relies primarily on a customer's self-certification. The collection process of BO information adds a huge burden on the financial institutions' operations. Additionally, the lack of publicly available UBO registry data remains a loophole in the entire AML effort. Complexity and broadness of the BO data is becoming one of the biggest challenges facing all the markets. It is crucial that compliance professionals take all reasonable measures to mitigate the risk associated with inaccurate, outdated beneficial ownership information.

Facing increased scrutiny of BO transparency, how can companies establish effective BO collection, identification and verification procedures to meet the expectations of regulatory and supervisory authorities? From an independent auditor's perspective, a separate audit project should be performed to manage the changes, evaluate the integrity and effectiveness of the compliance program with BO related regulatory obligations.

The objective of this white paper is to support discussions on addressing how the enterprise-wide risk assessment should be revisited, from an auditor's perspective. It also explores what best practices are needed to establish a robust beneficial ownership management program.

BACKGROUND

On January 13, 2016, The FinCEN issued Geographic Targeting Orders (GTO) that will temporarily require certain U.S. title insurance companies to identify the natural persons behind companies used to pay "all cash" for high-end residential real estate in the Borough of Manhattan in New York City and Miami-Dade County, Florida.

FinCEN is concerned that all-cash purchases – i.e., those without bank financing – may be conducted by individuals attempting to hide their assets and identity by purchasing residential properties through limited liability companies (LLC) or other opaque structures. "We are seeking to understand the risk that corrupt foreign officials, or transnational criminals, may be using premium U.S. real estate to secretly invest millions in dirty money," said FinCEN Director Jennifer Shasky Calvery.[1] Considering this GTO along with other BO related regulations released last year (many of them came in effective January 2016), we see two important signals: First, the center of AML/CFT scrutiny has been shifting from the entity level to the UBO level. Second, the regulators' attention has been expanded from the financial industry to Real Estate, Casino and other high risk arenas.

Why is it so important to know who may be hiding behind our customer? Companies and other legal structures that are anonymously owned and controlled are a key mechanism of global financial crime, tax evasion and corruption. Frequently such companies are also linked to international fraud, trafficking and even terrorist activities. Uncovering hidden BO is crucial to tackle tax evasion, money laundering and the terrorist financing, and to improve the health of the world economy.

> According to the World Bank, corrupt politicians used secret companies to obscure their identity in 70% of more than 200 cases of grand corruption surveyed by the World Bank.[2] Global detection rates of illicit funds by law enforcement are estimated to be as low as 1 per cent for criminal proceeds and the seizure rate is thought to be even lower, at 0.2 per cent.[3]

Every year, millions of new companies are registered with uncertain owners. In many jurisdictions, little or no identifying information is required to register an LLC or corporation. Formation agents set up shell companies which anyone can purchase online easily. Some secretive states such as Nevada, Wyoming, and Delaware have been dubbed "Shell Corporation Capitals" since they require little identifying information to incorporate. Companies also use complex ownership structures, trails of paperwork, and Bearer Shares/ Share Warrants (shares or right to acquire shares issued by a company which belong to whoever owns it) to conceal who is really in charge from the public.

With enhanced scrutiny by regulators, UBO identification and verification has become the essence of the client onboarding/ CIP process. This is not just a KYC, tax compliance or risk aggregation focus for financial institutions. The obligation impacts all industries with the Know Your Vendor (KYV)/ Know Your Third Party (KYTP) onboarding processes. This includes organizations requiring credit risk analysis, and other industries with relevant regulatory obligations such as real estate agents, dealers in precious metals and stones, lawyers, accountants and casinos.

REGULARTORY REQUIREMENTS

To be fully compliant with regulatory obligations, a deep understanding of the definition of Beneficial Owner is essential. It is surprising however that very few countries have defined the term Beneficial Owner in their domestic legislation.[4] In the countries which have a definition of BO, the definitions vary in scope and threshold. It is important that we acknowledge the differences.

BO disclosure is listed as a requirement in various regulatory documents in the US, UK and European Union. Financial Action Task Force (FATF) recommendations and some regulations such as FinCEN and the 4th EU Directive have listed requirements directly, while other regulations have indirectly indicated the BO information needs to be established. In this paper, we will review the ones with significant impact.

FATF: Beneficial owner is defined as the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement. Reference to "ultimately owns or controls" and "ultimate effective control" refer to situations in which ownership/ control is exercised through a chain of ownership or by means of control other than direct control.[5]

The CDD measures to be taken are as follows:

(a) Identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information.

(b) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is. For legal persons and arrangements this should include financial institutions understanding the ownership and control structure of the customer.

(c) Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.

(d) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

FinCEN CDD Requirements for FI - Final Rule: Beneficial Owner would include Each individual, if any, who, directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, owns 25 percent or more of the equity interests of a legal entity customer; and a single individual with significant responsibility to control, manage, or direct a legal entity customer or senior manager, including a Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, Managing Member, General Partner, President, Vice President, or Treasurer; or any other individual who regularly performs similar functions.[6]

4th EU AML Directive: In June 2015, the Fourth European Union Anti-Money Laundering Directive (the "Directive") came into force. Member States will have until 26 June 2017 to implement the Directive into national law. The Directive defines "beneficial owner" as any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted. With respect to corporate entities, a UBO is a natural person who ultimately holds a shareholding, ownership interest or controlling interest of more than 25% shares or voting rights in a corporate entity. If, after having exhausted all possible means and provided no UBO is identified, the natural person(s) holding the position of senior managing officials are, in principle, considered to be the UBO.

In the case of trusts and other legal arrangements, the settlor, the protector, if any, the beneficiaries and any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means, should be addressed as the UBO.[7] Article 13 specifically states that CDD measures shall comprise: "Identifying the beneficial owner and taking reasonable measures to verify that person's identity so that the obliged entity is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer…"

OFAC 50% rule: The rule, released in August 2014, states, "Any entity owned in the aggregate, directly or indirectly, 50% or more by one or more blocked persons is itself considered to be a blocked person."[8] This rule creates possibilities of unintentional violations where ownership information is difficult or impossible to obtain under certain circumstances. OFAC would expect that companies will apply reasonable due diligence measures to all business partners to reduce the risk of OFAC sanctions violations. For companies to accurately calculate the aggregated beneficial ownership, a 10% or 25% threshold may not be enough. Determining ownership as low as 1% to calculate the total ownership percentages across various owners may be required for the compliance officers to be confident.

FCPA/UK Bribery Law: From the anti-bribery/anti-corruption perspective, if a politically exposed person (PEP) is a beneficial owner in the subject company, or if the company is a state owned or controlled entity, there is a bribery/corruption risk in that business relationship. In addition, due diligence on higher risk entities may require examining beneficial owners to determine if they are on a sanctions/watchlist or pose adverse media or criminal concerns. Depending on their risk assessment, global companies (not necessarily financial institutions) may need to identify corporate upward linkage up to the global ultimate parent, as well as all the key principals at each level. This is to mitigate the risk of not knowing who they are doing business with.

FATCA: FATCA became law in March 2010, targeting tax non-compliance by U.S. taxpayers with foreign accounts. With respect to a corporation, a Substantial US Owner means any specified US person that owns, directly or indirectly, more than 10% of the stock of such corporation by vote or value. Comparable rules are provided for ownership in partnerships and trusts. For Foreign Investment Vehicles, the 10% ownership rule does not apply, which means an investment by a US person below 10% is reportable.[9] The law requires that each customer be classified into one of 30+ categories. The classifications demand very granular information on customers, especially entity customers.

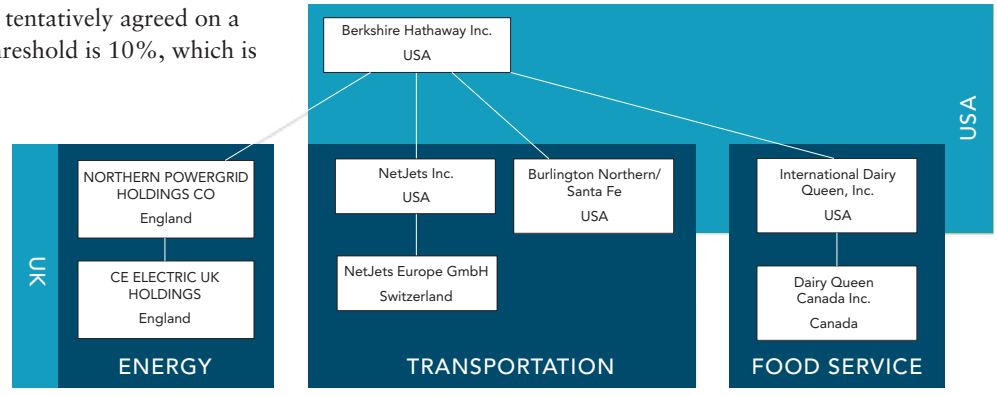
OECD CRS: The Common Reporting Standard (CRS), formally referred to as the Standard for Automatic Exchange of Financial Account Information, is an information standard for the automatic exchange of information (AEoI), developed in the context of the Organization for Economic Co-operation and Development (OECD). The legal basis for exchange of data is the Convention on Mutual Administrative Assistance in Tax Matters and the idea is based on the FATCA implementation agreements. On May 6, 2014, forty-seven countries tentatively agreed on a "common reporting standard"[10] The threshold is 10%, which is the same as FATCA.

Beside those direct requirements on Beneficial Ownership, other regulatory and supervisory authorities have also announced rules and requirements which will need accurate entity family structure and beneficial ownership data to understand the risk exposure.

Dodd-Frank: Section 766[11] of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd Frank") requires that the U.S. Securities and Exchange Commission (the "SEC") amend Section 13 of the Securities Exchange Act of 1934 (15 U.S.C.78m) to readopt reporting rules on beneficial ownership 13(d). Sections 13(d) and 13(g) require a person who is the beneficial owner of more than five percent of certain equity securities to disclose information relating to such beneficial ownership.

SEC new rule 506(e) disclosure:[12] On January 3, 2014, the SEC released a new set of Compliance and Disclosure Interpretations (C&Dis) relating to 20% beneficial owners. 506 (e) discloser requires Issuers to perform due diligence on any person that is going to become a 20% beneficial owner upon completion of a sale of securities. The beneficial ownership will need to be accurate, current and ready to be calculated at real-time.

BCBS 239: The Basel Committee on Bank Supervision published the, "Principles for effective risk data aggregation and risk reporting". Effective January 2016, banks should develop and maintain strong risk data aggregation capabilities to ensure that risk management reports reflect the risks in a reliable way.[13] The risk aggregation will require accurate and reliable beneficial ownership and reference data to establish entity family tree (hierarchy). Family Tree Linkage is the relationship between different companies within a corporate family which will allow accurate calculation on the accumulated exposure across the slices BCBS 239 identifies: legal entity ownership, industry, size and region.



GRAPH SOURCE: infoverity.com/

MiFID 2: Coming into force January 2017, the Markets in Financial Instruments Directive (MiFID) is EU legislation regulating firms providing services to clients linked to "financial instruments" and the venues where those instruments are traded. The regime for establishing position limits will impose significant burdens on investment firms and market operators in terms of monitoring compliance with such limits. It also imposes burdens on market participants who will have to provide information not only about their own positions, but also about those held by their clients, their clients' clients and so on to the ultimate owner of the position.[14] Again, the entity family tree data would be crucial here.

Market Abuse Directive (MAD II): An EU-wide framework for tackling both insider dealing and market manipulation. MAD II came into force on 2 July 2014. EU member states (with the exception of the UK) must transpose its provisions into national law by 3 July 2016. One of the indicators of market manipulation listed in the MAD Annex I is: Transactions that do not lead to a change in BO in the financial instrument or related spot commodity contract.[15] Once again, BO becomes a fundamental input into the entire control model.

Solvency II Directive (2009/138/EC): an EU Directive that codifies and harmonizes the EU insurance regulation. Primarily this concerns the amount of capital that insurance companies must hold to reduce the risk of insolvency. Solvency II needed to be implemented by January 1st, 2016.[16] The main challenges facing compliance staff are the lack of high quality, accurate data especially the entity ID and entity parent linkages.

THE CHALLENGES

Multiple regulations provide various BO definitions, threshold and due diligence requirements.

As reviewed in the regulatory section above, BO data has multiple dimensions. To determine who is the ultimate beneficial owner (UBO) we need to know whether the individual has ownership in shares or has control on voting; we need to know the percentage of such ownership or control; even if the ownership or voting right is lower than the threshold (i.e. 25%), other factors can still make this individual a UBO.

For threshold, in general KYC, KYV and AML, Anti-Bribery/ Anti-Corruption (ABAC) and CTF due diligence purpose, a BO of 25% or more is the threshold widely applied. Tax compliance and reporting, FATCA and CRS require a 10% threshold for ownership. For high risk customers, PEPs or for risk aggregation modeling, a lower threshold would be needed. In certain circumstances, entity ownership down to 1% or 0.01% is required.

In today's market, each financial institution faces more than one compliance and risk management requirement. Historically, firms often manage different compliance initiatives separately and business lines collect and maintain data separately. It is well recognized that outdated practices are not effective and may introduce additional risk to the company.

> How the BO data is collected, maintained and shared across the company and what definition and threshold should apply are important decisions for the leaders and stakeholders.

BO identification relies primarily on customers' self-certification

FATF is recommending a mechanism which establishes a combined approach for BO. The BO of an entity can be found in different places, including company registries, financial institutions, Trust and Company Service Providers (TCSPs), the legal person itself, and other national authorities, such as tax authorities, stock exchange commissions, or asset registries for land, property, vehicles, shares or other assets. However most of the sources are either only accessible for competent authorities or contain incomplete information.

For now the primary way to collect BO data is to have customers provide self-certification forms. The FinCEN NPR includes a standard certification form at Appendix A, which must be used by covered financial institutions to obtain beneficial owner information of legal entity customers. Further, FATCA offers a limited self-certification mechanism for account beneficial owners with Form W-8BEN and form W-8BEN-E. However, it is difficult to enforce the requirement that the customers accurately disclose BO information to the financial institutions. If the entity intends to hide the real beneficial owner, it can still conceal it. FinCEN does not require financial institutions to verify that the individuals listed as beneficial owners on the self-certification were actually the owners of the legal entity. This begs the question: how effective is the BO identification process if we only follow FinCEN's guideline? Without taking further steps to verify BO, financial institutions may not be fully compliant with laws and regulations implemented in other jurisdictions such as the 4th EU Directive.

From an operations perspective, many banks have the client fill out the forms manually and submit in person or via fax or email with the clerks entering the information into the computer system. For FATCA compliance, when W8 or W9 forms are required, it is overwhelming for both the customer and bank staff to handle all the information from different streams and various versions. Long turnaround time, postage costs and data management workload becomes a significant challenge for the bank to meet the reporting standard and timelines.

UBO data collection and accessibility at the central registry is the bottleneck for UBO identification and verification

The lead banking associations are broadly in favor of increased transparency around BO[17] and the strengthening of global AML/KYC standards, such as those set by the revised FATF recommendations, FinCEN and the 4th EU Directives. However, the significant lack of ultimate beneficial owner information collected at the states' or countries' central registry and lack of accessibility of this data to competent authorities and obligated entities remain the key loophole.

The FATF recommendations require, "Countries to ensure that adequate, accurate and timely information on the BO of corporate vehicles is available and can be accessed by the competent authorities in a timely fashion."[18] However, almost all FATF countries will struggle to implement a central registry in national law and build the program to meet this requirement. In the majority of countries, there is typically no requirement to disclose the true owner's names if the names listed are just nominee shareholders and directors. It will take years before we can see the light. Here is the current status:

– The G-8 core principles[19] make clear that a company should know who owns and controls it and its BO. "Basic information about the company should be adequate, accurate, and current. BO information on companies should be accessible onshore …… This could be achieved through central registries of company beneficial ownership and basic information at national or state level." The U.K. will become the first country in the world to operationalize a public register of BO information. Companies were required to hold their own "persons with significant control" (PSC) register from January 2016. From April 2016 they will have to give this information to Companies House when they deliver their confirmation statement (which replaces the annual return). This means that Companies House will hold PSC information for all the UK companies in scope by April 2017. Companies House will make all the PSC information available for free in one central, searchable public register.[20]

– In May 2015, the EU also finalized a measure that, among numerous provisions, requires all EU member states to create central registries of BO information for companies established in their countries by 2017.[21] The EU states are not explicitly asked to make the registries public, as long as the information can be made available to people with "legitimate interests." The states can choose to make the information public or not.

– The U.S. has made positive commitments to tackle anonymous companies in recent years. However, it has failed to pass the Transparency and Law Enforcement Assistance Act - a bill requires U.S. states to collect BO information on companies formed in their state and to make the information accessible to law enforcement. Certain US states are still considered to maintain high levels of secrecy for anonymous entity vehicles, such as Nevada, Wyoming, and Delaware. According to the recent ranking published by Arachnys (a digital research platform), the US currently ranks No. 45 in terms of the ability to access information on companies. This is below Russia (No. 1), India (No. 9), Jordan (No. 11), and Thailand (No. 44).[22]

– The G-20 also took a step forward at the Brisbane Summit in November of 2014 by recognizing the importance of collecting BO information in their High Level Principles on Beneficial Ownership. Some other countries such as Ukraine launched its registry in October 2014 and reformed the process of business registration at the end of 2015. Japan announced a revision of AML law in June 2015, namely the "Act on Prevention of Transfer of Criminal Proceeds (APTCP)", which is intended to catch up with FATF recommendations on Beneficial Ownership.

– The Extractive Industries Transparency Initiative (EITI) has launched a BO pilot which seeks to make extractive companies' BO available to the public. Eleven EITI countries are now taking part in the pilot and will disclose the identity of the real owners of the extractive companies operating in their countries.[23]

Complexity and breadth of BO data is the greatest challenge facing all stakeholders.

To hide the true ownership or control of front companies, the criminals would deliberately try to create multiple layers of ownership using complex but legitimate corporate structures spanning various borders. This makes the money movement and ownership almost untraceable. A typical financial firm may have a large customer base with the BOs across a hundred countries, using dozens of different local languages; making the BO reference data identification and verification extremely difficult. It is expensive, risky and inefficient to establish an accurate customer ownership structure in-house, let alone periodically refresh the BO data to keep it current.

It's challenging regardless which way you go, either via the UK/EU approach by building a central registry or the US approach to reply solely on customers' self-certification.

No-one can escape the expected compliance obligations while waiting for the countries' central registry to be ready and available to public, neither can you solely rely on the customer's self-certification on BO without taking all reasonable measures to verify and investigate, especially when on-boarding customers with a higher risk level. Bottom-line is that the enterprises must know who the real customer they are dealing and appropriately apply controls on the risks.

HALLMARKS OF A ROBUST BO PROGRAM

Executives, compliance officers and auditors need to evaluate and adjust their existing practices on BO management to changing regulations and environments. This will enable them to represent to regulators that they have expended best efforts to establish BO on their customers. Financial institutions need a well-designed BO management program, integrated into their existing enterprise-wide compliance program. This program should not interfere with existing functions. The solution should demonstrate the firm's compliance program has exhausted "all reasonable measures"[24] to identify and verify the beneficial owner of the existing and new customers. Moreover, the stakeholders should make the best effort to implement the program with the organization's financial and human resources. A robust ultimate BO management program should:

Follow the FATF AML framework: The program should manage the full BO data governance life-cycle and should be integrated into each component of the entire compliance program which includes policies, procedures, and risk assessment, due diligence, reporting, record-keeping, and training, culture, independent testing and audit.

Embrace a risk-based approach: Implement a reasonable risk assessment process to evaluate how the BO data as a factor would impact the customer risk profile as well as the overall enterprise-wide compliance and audit risk assessment. The risk level elevation should lead to a deeper due diligence, require a higher level of approval and more closed monitoring, testing and auditing.

Utilize a combination of the best available mechanisms: Adopt a combination of the best available mechanisms which includes a customer's self-certification, integrating/cross referencing with the registry or reputable partner's quality BO data with the addition of adverse media and open source findings for enhanced due diligence.

Centralize the enterprise-wide BO structures to meet all compliance and business needs: Have the capability to share and obtain BO information across the enterprise and associated affiliates. Ideally, it should allow automated regulatory reporting based on self-configured ownership.

There is no one-size-fits-all solution. Each institution should take an appropriate approach commensurate to the organization's risk profile. One of the best approaches is to have independent auditors give the existing compliance program a thorough evaluation on the effectiveness and integrity regarding beneficial ownership compliance benchmarking with all applicable, recent regulations.

AUDIT CONSIDERATIONS

Knowing many new laws became effective in and around January 2016, compliance officers and auditors need to carefully assess the risks associated with these new BO regulations within the organization and implement practical changes to build a robust BO management program.

From an independent auditor's perspective, the BO regulation changes should be managed as a separate project. Auditors would expect compliance to evaluate the integrity and effectiveness of the compliance program in regards to BO related regulatory obligations. Compliance needs to address how the enterprise-wide risk assessment should be revisited as well as what best practices are needed to establish a robust BO management program.

AML & AUDIT RISK ASSESSMENT

Compliance should revisit BO-related enterprise-wide AML risk assessment

Before looking into details of how the process should be changed, it is crucial to first conduct an enterprise-wide AML risk assessment to identify the gaps in existing controls, policies, procedures and processes. This helps ensure compliance with all applicable BO related regulatory guidance and expectations. Fine-tune the AML risk assessment when appropriate.

An independent auditor or compliance officer can start the risk assessment with the following questions:

- Which regulatory obligation is the entity exposed to (especially those newly announced)?
- How are these obligations related to BO?
- What threshold is required for each of these BO requirements?
- In addition to the AML department, does any other department such as credit and risk also require BO information? Within each involved department, the following questions should be asked:
    - When or at which stage of a business relationship is BO data is collected/used?
    - Who in the company is responsible for such tasks?
    - Is any outsourced data or service adopted? Has any risk evaluation been performed when choosing the third-party data?
    - How is the BO currently identified and verified? Are they properly documented?
    - How frequently is the BO information refreshed/ reviewed and what are the triggers for review? Is the BO information change monitored?
    - How long are the BO- related records kept on file?

- Is the BO information shared with any other department?
- What is the escalation process if the required BO information is missing or inaccurate?

– How would the quality/availability of BO information impact the customer risk evaluation?

– How is the BO information shared and reconciled internally among different departments?

Detailed analysis should be performed based on the answers collected, the gaps in the controls should be identified and the changes should be clearly recommended.

The enterprise-wide AML compliance risk reassessment should consider how the BO/UBO risk is being managed and controlled throughout the entire compliance program, including policies and procedures, risk ranking, customer due diligence, reporting, record-keeping, on-going monitoring, internal control and auditing, etc.

An auditor should spend quality time to evaluate compliance regarding the risks assessment and controls on customer risk model and the risks brought in by third-party data provider. An auditor would expect that:

Compliance should bring BO data risk into the customer risk evaluation model.

Previously, BO information may not have been a mandatory data element in the CIP process and may not have been highlighted as a key factor in the existing customer risk model. It is also likely that the BO data management obligations and controls were not considered as a separate factor in the overall compliance risk assessment. With recent increased regulatory scrutiny, BO management practices should be incorporated into each relevant risk assessment model/tool.

> As one component of the enterprise-wide AML risk, a BO risk assessment should use the consistent rating measurements and quantitative values that are used in the overall AML, ABAC and sanctions risk assessment. For example, a high, medium, low or a red, amber, green ranking or 0-9 scores. This ranking or score should plug seamlessly into the institution's total AML, ABAC and sanctions risk rating model.

Institutions should incorporate the BO data availability and quality into the existing customer risk rating. Compliance could add or adjust some factors to their existing risk model which include:

– Geography: An evaluation of the country's risk level should consider its legislation on BO data disclosure, BO information collection at a central registry and whether such registry data is publicly available. This assessment will be a different country risk from the existing country risk index we use for AML or anti-bribery/anti-corruption compliance.

– Completeness and accuracy: How complete are the self-certification forms and how accurate are they from an initial verification process? *For details, see the verification process in a later section.*

– Customer type: The weight of customer type input should be adjusted in the existing risk assessment model considering the new BO requirements from the new regulations. I.e. a publicly listed company vs. a limited liability company vs. a trust.

– BO change flag: Any sign/flag that shows the BO information has been changed or is going to change. Such flag can be received via media search/monitoring tool with search strings, such as M&A, IPO, insolvency, name changes etc.

> The BO impact in customer risk level will lead to an elevation on the level of due diligence needed, a requirement for a higher approval level and/or closer monitoring. If significant residual risk exists, a SAR may need to be filed and a de-risking measure will need to be implemented.

Compliance should evaluate third party data provider risk before adopt any external data. It should also regularly review the third party data risks.

If an independent data provider is introduced into the BO data management program, then the compliance department should assess the third party risk associated with BO and entity ownership structure data. Also effective controls should be implemented. An auditor will review the risk assessment and control measurements during the independent audit.

Auditors would expect the following questions to be asked and the answers to be collected, analyzed and documented properly:

– Data accuracy and granularity: How accurate is the entity ownership structure? Does it cover all the layers up to global ultimate parent? What is the percentage of ownership we can trace, 0.01%, 1% or 10% or 50%?

– Data freshness: How frequently is the data refreshed and what triggers the refresh?

– Data coverage: How many geographic regions can the third party data provider cover? What is the percentage of entities covered in each region compared to the total number of registered entities? Is there any significant gap in the coverage?

– Data security: How is the data transferred between the third party data provider and our organization? How is our data handled and stored within the provider organization? Will there be any risk associated with data privacy, confidentiality breach, or other security risk?

– Legitimacy, consistency and reliability: What are the data origins and collection method? Is the process/procedure legitimate and reasonable? How concisely is the procedure being followed? Does the third party have a compliance program in place?

– Stability: How long has the third party data provider being in business? What is the data provider's size, reputation, financial performance? Is the contract a monthly or long-term strategic partnership and is a similar data provider easily accessible in case of BCP?

THE COMPONENTS OF A ROBUST BO/UBO PROGRAM

Auditors will review if the policy, procedures are updated to clearly define Beneficial Owner and the threshold.

The enterprise should consider updating the policies and procedures to clearly define Beneficial Owner and Ultimate Beneficial Owner and also set the threshold to meet the most recent and highest regulatory obligations. If the enterprise is operating in multiple jurisdictions (probably in most of the cases), the highest level of BO-related regulatory requirements should be used.

Compliance officers should maintain control of the regulatory changes and proactively refresh the practices to meet changing regulations. Auditors would want to see:

– Evidence showing that compliance officers have tools/ methods to keep up with ongoing changes;

– A log to categorize all the relevant BO regulations and requirements and why it's applicable to the enterprise;

– The reasonable and persuasive means lead to the definition and threshold decision.

> For instance, if a financial institution is subject to compliance with both FATCA and BSA/AML, a BO data collection process should meet the higher standard from FATCA which will require a 10% threshold (or lower) instead if FATF requirement of 25%.

Auditors will validate if the BO data collection, storage and sharing process are consistent and streamlined.

If the same ownership data set has been collected at different business stages, by different departments, this would constitute a deficiency in the process. An opportunity would exist to gain efficiency by centralizing the BO information collection point and moving the process upfront. If the data is collected and centralized at the beginning of the business relationship, it is much easier for compliance staff and business units to share and utilize the data. Customers would appreciate the efficiency and the organization would benefit from increased cost effectiveness. Further, as we will discuss in a later section, the single point of data collection benefits future data integration and refreshment.

When considering whether to centralize BO information and share such information for internal use, it is important that the domestic and foreign data privacy laws should be carefully reviewed by legal counsel. To what extent the BO data can be shared and to whom in which way - all these decisions should be backed up with legal review and the appropriate customer disclosure or consent. Once implemented, an auditor will need to validate how these process are executed and if there is any violations.

Auditors will review the BO data reconciliation process and the methods used to decide BO confidence level.

Enterprises cannot rely solely on customer self-certification. One of the best options is to compare the UBO information collected with the country's central registry data when available or with a reputable integrated data provider's data. The reconciliation process should be well designed, documented and executed. Auditors would ask questions such as:

– Has a reconcile process been established? How often is it scheduled?

– What is the data source used to reconcile? What is the status of the data availability?

Auditor's tips: Data source selection

Whenever the central registry data is available or accessible, such data should be utilized to identify the entity and its BO formed in that country. Such data can be inquired directly from the country's registry or can be provided by a third party data provider who has the right to distribute such data in an accurate and current manner. Assuming countries will roll out the central registry at different times, it can be difficult for financial institutions to keep tracking the status and figure out the inquiry mechanism in all countries. The local language capability could be another obstacle. Using a reputable third party data provider is a good way to insure the capture of required BO data. In addition, for Customers in countries which don't have a public central registry available, properly integrating quality reference data from a reputable third party data provider would be the next best available option.

Financial institutions could utilize a third party data provider's comprehensive commercial database and ownership structures (linkages) to help establish its own beneficial ownership structures, identify and verify the UBO and review associated parties such as principals, key customers, layers of parents etc. Such data can be accessible by individual inquiry via software-as-a-service (SaaS) application or bulk match and data append via application programming interfaces (APIs) or SFTP batch feed.

Third party data append could help visualize the full scope of your customer. When customers disclose their beneficial ownership to financial institutions, they often only provide the minimum and mandatory information, even if based on their best knowledge. However a data provider will be able to show the entire family network: the customer itself, all layers of parents up to global ultimate, subsidiaries and affiliates, key principals. It will also include key customers of customers which help understand the customer's BO and control. All of which is useful to calculate the aggregated exposure.

Data providers have expertise in all geographic regions, meeting both local data privacy laws and international legal standards. Some data providers have been collecting business information for many years. For example, Dun & Bradstreet (D&B) has been in business for 170 years. D&B gathers data from 30,000 data sources in over 200 countries, owning +280 million entity records and 19 million global linkages.[25] *The database is refreshed over 1.5 million times a day. Whether the customer is a tiny private entity or a giant publicly listed entity, whether it is located in the US, in Far East or Africa, with a complex ownership structure, reliable data will give you the confidence to make compliance decisions. Such capability is unmatchable with any financial institution's in-house data collection.*

– What is the process for reconciling differences?

– What are the protocols when information can't be obtained or reconciled?

– What are the situations where escalations are necessary?

– What level of approval is required for different *scenarios?*

– How the reconciliation results are reported? Any statistics metrics adopted?

Auditor's tips: Reconcile basics

When BO data from the two sources match, the BO risk should be considered as lower risk (please note, this is the BO risk indicator only, not the entire customer risk) and the basic verification and due diligence process should additionally be performed.

If the two data sets are partially matched and verified, the BO risk indicator will be medium. Reconciliation with the customer is required.

If the two data sets are totally irrelevant, raise the BO risk indicator to high, and reconcile with the customer. If there is enough evidence showing the customer was hiding the real UBO intentionally, raise the BO risk to high. The high risk level will lead to further action such as enhanced due diligence, termination of the relationship, higher level of approval etc. in certain case, a SAR may need to be filed on this customer.

When the BO risk indicator is medium or high, institutions should consider conducting a deeper level of due diligence, adding adverse media/open source search and screening additional relevant entity names to mitigate the risk. The names to be screened should include all the parent entities and their key principals. Also the recertification cycle should be shorter (i.e. every six months) on these high risk customers.

Auditors will validate how the BO changes are monitored.

After the on-boarding, whenever it is feasible, institutions should continually monitor the possible ownership changes to existing customers. Auditors will validate if alerts are received promptly on events such as M&A linked ownership change, name change or significant management changes. They will also monitor how the changes are found from which channel. Is it from customer self-reported ownership changes, annual recertification program, data provider's database updates or from media/open source search results? Once the alert is received, has the customer's profile been reviewed and BO information been recertified?

CONCLUSION

Building a robust BO/UBO management program is crucial to allow compliance practices to adapt to increased BO scrutiny. BO/UBO identification and verification is not only an obligation for financial institutions on KYC, AML, tax, sanctions compliance or risk aggregation requirements, but the scrutiny has also been expanded to include many industries' onboarding processes. It has even been extended to organizations that require credit risk analysis, and are exposed to other relevant regulatory obligations such as real estate agencies, dealers in precious metals and stones, lawyers, accountants and casinos.

To help compliance professionals overcome the challenges from complex corporate structures, limited public registry data and increased scrutiny of BO, this white paper began by exploring the current BO related guidance and regulations, analyzing the BO related challenges and then highlighting the hallmarks of a robust BO program. It also provides practical recommendations from an auditor's perspective.

Auditors would recommend the BO regulatory changes be managed as a special project.

First, compliance officers/auditors should revisit enterprise-wide AML and audit risk assessment, ensure that the BO related risk is thoroughly assessed and controlled in each piece of the entire compliance program. Especially, special attention should be given to the customer risk evaluation model and the risks associated with adopting third party BO data.

Second, auditors would also expect the compliance program to manage the development of a robust BO/UBO program:

– The BO/UBO program should take a risk-based approach.

– The policy and procedures should be updated to clearly define BO and the threshold.

– The BO data collection, storage and sharing process should be consistent and streamlined.

– The BO data reconciliation process and the methods used to decide BO confidence level should be carefully designed and controls should be implemented to ensure the sound execution.

– The BO changes monitoring process should be implemented and valid.

Finally auditor's best practices are shared about how to utilize hand-picked, best available methods and data sources to empower the identification, verification and reconciliation.

A robust BO/UBO management program should consider these auditor's recommendations and hallmarks to help mitigate the risks raised from the increased BO scrutiny. Adopting these best practices would help the stakeholders to demonstrate to the auditors and regulators that the best efforts have been given and all reasonable measures have been utilized to establish a comprehensive BO strategy.

REFERENCES

1 Financial Crimes Enforcement Network, January 2016: https://www.fincen.gov/news_room/nr/html/20160113.html

2 World Bank: Stolen Asset Recovery Initiative, October 2011, https://star.worldbank.org/star/publication/puppet-masters

3 UNODC, "Illicit Financial Flows" 2011.

4 OECD http://www.oecd.org/ctp/treaties/BENOWNMLL_vanBladel.pdf

5 FATF Recommendations 2012: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

6 FinCEN Customer Due Diligence Requirements for Financial Institutions; Final Rule 2016: https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf

7 DIRECTIVE (EU) 2015/849: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L0849

8 OFAC https://www.treasury.gov/resource-center/sanctions/Documents/licensing_guidance.pdf

9 https://files.dlapiper.com/files/Uploads/Documents/FATCA-Alert.pdf

10 Wikipedia: https://en.wikipedia.org/wiki/Common_Reporting_Standard

11 Dodd Frank Act Section 766, 2010 http://www.dodd-frank-act.us/Dodd_Frank_Act_Text_Section_766.html

12 New Rule 506 FAQs, January 2014 http://dodd-frank.com/new-rule-506-faqs-20-beneficial-owners-506e-disclosure/

13 same as 12

14 Freshfields Bruckhaus Designer: http://www.freshfields.com/uploadedFiles/SiteWide/Knowledge/00468_PG_COR_MiFID%202%20Commodities%20Briefing_AW3.pdf

15 Esma Consultation Paper, July 2014 ESMA/2014/808 www.esma.europa.eu

16 WIKIPEDIA https://en.wikipedia.org/wiki/Solvency_II_Directive

17 https://www.transparency.it/wp-content/uploads/2014/05/TI-G20-Position-papers-Beneficial-Ownership.pdf

18 FATF Guidance: Transparency and Beneficial Ownership, October 2014

19 G8 Action Plan Principles to prevent the misuse of companies and legal arrangements https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/207532/G8-Action-Plan-principles-to-prevent-the-misuse-of-companies-and-legal-arrangements.pdf

20 http://www.lowtax.net/features/The-UKs-Registry-of-Beneficial-Ownership-573292.html

21 Global Financial Integrity, June 2015 http://www.gfintegrity.org/norway-latest-country-to-adopt-public-registry-of-beneficial-ownership/

22 Global Rankings by Arachnys: https://compass.arachnys.com/rankings

23 Pilot project: Beneficial Ownership: https://eiti.org/pilot-project-beneficial-ownership

24 FATF Recommendations 2012: http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

25 The World's Most Comprehensive Commercial Data Base http://www.dnbsame.com/company/global-data-coverage/