NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA 22314

DATE: August 2018 **LETTER NO:** 18-CU-02

TO: Federally Insured Credit Unions

SUBJ: Examination Guidance for Bank Secrecy Act Customer Due Diligence and Beneficial Ownership Compliance

ENCL:
- Supervisory Letter – Bank Secrecy Act Customer Due Diligence and Beneficial Ownership Rules
- BSA – Questionnaire
- Customer Due Diligence and Exam Procedures – Overview
- Beneficial Ownership Requirement for Legal Entity Customer – Overview

Dear Board of Directors and Chief Executive Officer:

The NCUA issued examination procedures to field staff regarding customer due diligence and beneficial ownership provisions that are part of the Bank Secrecy Act/Anti Money Laundering Rules (BSA/AML). The attached supervisory letter provides all federally insured credit unions with the examination expectations provided to the NCUA examiners regarding the review of a credit union's compliance with these areas. This includes new examination procedures that will be incorporated into the Federal Financial Institutions Examination Council (FFIEC) *Bank Secrecy Act/Anti-Money Laundering Examination Manual*. To further assist you, the NCUA has consolidated BSA resources for credit unions on the NCUA website.[1]

As noted in prior updates from the NCUA, effective May 11, 2018, credit unions are required to comply with new BSA/AML rules the U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) published on May 11, 2016 (*Customer Due Diligence Requirements for Financial Institutions*). The rules are intended to codify customer due diligence requirements for covered financial institutions. They contain a new requirement for such institutions to identify and verify the identity of individuals (the beneficial owners) who own or control certain legal entity members, subject to a number of exclusions and exemptions.

The NCUA recognizes that some credit unions may need additional time to implement changes and to fully comply with the new requirements. The NCUA examiners have been instructed to accept a credit union's reasonable and good faith efforts to comply with the new rule throughout 2018. However, credit unions should understand that the NCUA's acceptance of good faith efforts for supervision purposes does not shield a credit union from FinCEN penalties that could arise from failing to comply with all BSA/AML requirements.

If you have any questions regarding this letter, please contact your regional office or state supervisory authority.

Sincerely,

/s/

J. Mark McWatters

Chairman

---

[1] See https://www.ncua.gov/regulation-supervision/Pages/bank-secrecy-act.aspx

Last modified on 06/15/20

Supervisory Letter

NCUA | Office of Examination & Insurance
1775 Duke Street, Alexandria, VA 22314
www.ncua.gov

SL No. 18-01
August 17, 2018

TO: **All Field Staff**

SUBJECT: **Bank Secrecy Act Customer Due Diligence and Beneficial Ownership Rules**

ENCL:
1) Customer Due Diligence – Overview and Examination Procedures
2) Beneficial Ownership Requirements for Legal Entity Customers – Overview and Examination Procedures
3) Bank Secrecy Act Questionnaire

This supervisory letter provides information about the Bank Secrecy Act (BSA) customer due diligence (CDD) and beneficial ownership rules, and establishes a consistent framework for the examination and supervision processes used to evaluate credit union compliance. The guidance in this document applies to all federally insured credit unions (FICUs).

I. Background

The U.S. Department of Treasury's Financial Crimes Enforcement Network (FinCEN) issued final rules under the BSA on May 11, 2016, published as *Customer Due Diligence Requirements for Financial Institutions* in the Federal Register.

The rules strengthen and codify existing CDD requirements for covered financial institutions, and they contain a new requirement for such institutions to identify and verify the identity of individuals (the beneficial owners) who own or control certain legal entity members, subject to a number of exclusions and exemptions. FICUs and other covered institutions must comply with the rule, effective May 11, 2018.

This supervisory letter provides field staff with guidance regarding expectations and the implementation of examination procedures to review compliance with the new rules.

Supervisory letters are official agency examination policy. These letters communicate guidance to NCUA field staff on regulations and exam procedures. Each supervisory letter focuses on a specific topic, providing background information and outlining any related regulatory and statutory requirements. Supervisory letters may also require field staff to perform certain procedures during an examination; in these cases, the letter will provide instructions to help field staff implement the procedures. Supervisory letters are intended to provide a framework for more consistent application of staff judgment with respect to conclusions about a credit union's financial and operational condition, and related CAMEL and risk ratings. These letters also provide a consistent approach for evaluating the adequacy of a credit union's relevant risk-management processes. Supervisory criteria detailed in a supervisory letter are not strict requirements, unless noted as required by law or regulation. The supervisory criteria contained in these letters are used by field staff to evaluate a credit union's condition based on the preponderance of relevant factors. Generally, supervisory letters are shared with the public as an attachment to a Letter to Credit Unions.

II. BSA/Anti-Money Laundering (AML) Programs

Together, CDD and beneficial ownership requirements are now a required minimum component of a credit union's BSA/AML internal controls.[1] The four pillars of a BSA/AML compliance program include:

1. System of internal controls to ensure ongoing compliance, including appropriate, written risk-based procedures to:
    - Understand the nature and purpose of the member relationship in order to develop a member risk profile, and conduct ongoing due diligence to identify and report suspicious transactions; and
    - Identify and verify the identity of beneficial owner(s) of legal entity members, regardless of risk profile, for each new formal banking relationship established on or after May 11, 2018.[2]
2. Independent testing of BSA/AML compliance
3. Individual responsible for day-to-day compliance
4. Training for appropriate personnel

III. Examination Expectations

The updated BSA Questionnaire is attached to this letter to give you a preview of the new CDD and beneficial ownership questions. Once the updated BSA Questionnaire and Consumer Compliance Violations citations have been added to AIRES, which is expected with the September 2018 release, field staff will begin evaluating a credit union's compliance with the final CDD and beneficial ownership rules. Initially, NCUA field staff will discuss and determine a credit union's awareness of, and review its efforts to comply with, the new requirements.

IMPORTANT: Throughout the remainder of 2018, NCUA field staff will not take exception to a credit union's non-compliance with the new BSA standards found in FinCEN's final CDD and beneficial ownership rules effective May 11, 2018, and will not identify any such non-compliance as a significant BSA violation, **provided the credit union is making a good faith effort to comply with the new rules**.

---

[1] The NCUA and the other federal financial institution regulators consider CDD and beneficial ownership requirements to be an essential part of a financial institution's internal control processes and procedures, but you may hear these requirements referred to as a "fifth pillar."

[2] A beneficial owner is an individual (natural person) who, directly or indirectly, owns 25 percent or more of the equity interests of a legal entity member (ownership prong); or an individual with significant responsibility to control, manage, or direct a legal entity member (control prong).

In 2019, NCUA field staff will begin more in-depth reviews of credit unions' BSA/AML policies, procedures, and processes in order to assess their overall compliance with regulatory requirements for CDD and for identifying and verifying beneficial owner(s) of legal entity members.

The NCUA partnered with the other Federal Financial Institutions Examination Council (FFIEC) agencies to develop the enclosed guidance and examination procedures, *Customer Due Diligence – Overview and Examination Procedures* and *Beneficial Ownership Requirements for Legal Entity Customers – Overview and Examination Procedures*.[3] The new guidance is included in the enclosed, updated BSA Questionnaire and will be incorporated into the FFIEC *Bank Secrecy Act/Anti-Money Laundering Examination Manual*.[4] NCUA field staff will review and become familiar with these procedures before examining a credit union for the new rule requirements.

FinCEN issued an administrative ruling concurrent with the release of the interagency guidance documents, providing an exception for premium finance lending products that allow for cash refunds. Specifically, Ruling FIN-2018-R001, *Premium Finance Cash Refunds and Beneficial Ownership Requirements for Legal Entity Customers*, provides exceptive relief to covered financial institutions from the requirements to collect and verify the beneficial owner of a legal entity customer opening such premium financing account when there is a possibility of a cash refund. There is no expiry date on this exceptive relief.

In addition, FinCEN issued an administrative ruling on May 16, 2018, to provide 90-day limited exceptive relief from the obligations of the beneficial ownership requirements. Specifically, the ruling applies to certain financial products and services that automatically roll over or renew (such as share certificate or loan accounts) and were established before the rule's applicability date of May 11, 2018. On August 8, 2018, the limited exception was extended an additional 30 days. See FIN-2018-R002, *Beneficial Ownership Requirements for Legal Entity Customers of Certain Financial Products and Services with Automatic Rollovers or Renewals*, and FIN-2018-R003, *Extension of Limited Exception from Beneficial Ownership Requirements for Legal Entity Customers of Certain Financial Products and Services with Rollovers and Renewals*, for more information about the applicability of these rulings.

IV. Additional Guidance Relevant to BSA CDD and Beneficial Ownership Rules

Previously issued guidance on CDD and beneficial ownership includes:

[3] See https://www.fincen.gov/resources/statutes-and-regulations/cdd-final-rule for more information and guidance on complying with the CDD final rule and beneficial ownership identification and verification requirements.
[4] See the BSA/AML InfoBase, available on the FFIEC's website at https://www.ffiec.gov/supervisory.htm.

- FinCEN Frequently Asked Questions
    - FinCEN Guidance FIN-2018-G001, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions* (April 3, 2018)
    - FinCEN Guidance FIN-2016-G003, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions* (July 19, 2016)

- Webinars[5]
    - NCUA Office of Credit Union Resources and Expansion (CURE) webinar, *BSA Compliance – Customer Due Diligence* (April 25, 2018)
    - FFIEC interagency webinar, *Examiner Training for Customer Due Diligence and Beneficial Ownership Examination Procedures* (April 19, 2018)

If you have any questions about the information in this letter, please direct them to your immediate supervisor or your regional management.

Sincerely,

/s/

Larry Fazio
Director
Office of Examination & Insurance

Enclosures (3)

[5] The archived CURE webinar is available through NCUA's Credit Union Learning Management Service. The FFIEC webinar will be shared internally with NCUA staff.

BSA - Bank Secrecy Act

INTRODUCTION AND PURPOSE	
REPORTS	
PENALTIES	
RECORD RETENTION REQUIREMENTS	
REGULATORY REFERENCES	

		Yes/No/NA	Comments
Risk Assessment / Scoping			
1.0.0	Does review of the AIRES Compliance Violations module indicate that all prior violations are resolved?		
2.0.0	Has the credit union received correspondence from law enforcement or outside regulatory agencies relating to BSA compliance since the last examination?		
3.0.0	Does the credit union maintain a list of high risk accounts?		
4.0.0	Has the credit union completed an appropriate assessment of BSA AML risk?		
4.0.a	Assess BSA risk using examiner judgment and note exam BSA risk assessment in Comments box.		
Basic Requirements - Policy			
5.0.0	Has the board of directors established an appropriate written program to assure the CU meets BSA reporting and recordkeeping requirements?		
	Does the written BSA compliance program address:		
5.0.a	Internal Controls (748.2(c)(1))		
5.0.b	Independent Testing (748.2(c)(2))		
5.0.c	Responsible Individual (748.2(c)(3))		
5.0.d	Training (748.2(c)(4))		
5.0.e	Customer Identification (748.2(b)(2))		
5.0.f	Customer Due Diligence (1020.210(b)(5))		
5.0.g	Beneficial Ownership Identification and Verification (1010.230(b))		
Basic Requirements - Practice			
6.0.0	Has the credit union established an adequate Customer (member) Identification Program (CIP)? (1020.220)		
6.0.a	Does the CIP require the minimum information (name, date of birth, address, identification number) prior to opening an account? (1020.220(b)(2))		
6.0.b	Does the CIP require verification of the information obtained? (1020.220(b)(2))		
6.0.c	Does the CU have a process for handling exceptions to the standard CIP policy?		
6.0.d	Does the CU keep CIP data for five years after account is closed and CIP documents for, at least, five years after account is opened? (1020.220(b)(3)(ii))		
6.0.e	Does the CU provide adequate member notice it is requesting information to verify their identity? (1020.220(b)(5))		
7.0.0	Has the CU established an adequate Customer (member) Due Diligence (CDD) Program? (1020.210(b)(5))		
7.0.a	Does the CU have effective procedures for developing member risk profiles that identify the specific risks of individual members or categories of members? (1020.210(b)(5)(i))		
7.0.b	Are the risk-based CDD policies, procedures, and processes commensurate with the CU's BSA/AML risk profile, with increased focus on higher risk members? (1020.210(b)(5)(i) and (ii))		

		Yes/No/NA	Comments
7.0.c	Do procedures include identifying members that may pose higher risk for money laundering or terrorist financing and whether and/or when, on the basis of risk, it is appropriate to obtain and review additional member information? (1020.210(b)(5)(i) and (ii))		
7.0.d	Has the CU developed procedures for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained?		
7.0.e	Do policies contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a member's risk profile, as applicable?		
7.0.f	Has the CU developed procedures for performing ongoing monitoring of the member relationship, on a risk basis, to maintain and update member information, including beneficial ownership information of legal entity customers/members? (1020.210(b)(5)(ii))		
7.0.g	Has the CU defined in its policies and procedures how member information, including beneficial ownership information for legal entity customers/members, is used to meet other relevant regulatory requirements, including but not limited to, identifying suspicious activity and determining OFAC sanctioned parties? (1020.210(b)(5)(ii))		
8.0.0	Has the CU established written procedures, included in their BSA/AML compliance program, that are reasonably designed to identify and verify beneficial owners of legal entity customers/members? (1010.230(a))		
8.0.a	Do the CU's procedures require identification of the beneficial owner(s) of each legal entity customer/member at the time a new account is opened on or after May 11, 2018 (unless the member is otherwise excluded pursuant to paragraph (e) of this section or the account is exempted pursuant to paragraph (h) of this section)? (1010.230(b)(1))		
8.0.b	Do the CU's procedures require the minimum information (name, address, identification number, and data of birth) for beneficial owner(s) of legal entity customers/members, and timely verification of enough information to form a reasonable belief as to the beneficial owner's true identity? (1010.230(b)(2))		
8.0.c	Does the CU have a process for circumstances in which it cannot form a reasonable belief that it knows the true identity of the beneficial owner(s) of a legal entity customer/member?		
8.0.d	Does the CU retain a record of the identity information, the method used to verify identity, and verification results for the required period? (1010.230(i))		
9.0.0	Is the credit union's independent testing adequate for the size and complexity of the institution? (748.2(c)(2))		
10.0.0	Does the BSA officer have appropriate knowledge, resources, and authority - commensurate with the complexity of the credit union's operations? (748.2(c)(3))		
11.0.0	Is the credit union's training adequate for the size and complexity of the institution? (748.2(c)(4))		
Reporting - Data Quality Violations			

		Yes/No/NA	Comments
10.0.0	Does the credit union have an adequate process to identify transactions that require completion of a Currency Transaction Report (CTR)? (1020.311)		
10.0.a	Since the prior exam, have one or more transactions occurred that require reporting through a Currency Transaction Report (CTR)?		
10.0.b	Does the credit union electronically file a CTR with FinCEN for all currency transactions greater than $10,000 (1010.311), and multiple transactions in currency which aggregate to more than $10,000 occurring in one day (1010.313) , unless it is an exempt transaction?		
10.0.c	Is the CTR filed within 15 days after the transaction occurs? (1010.306)		
10.0.d	Does the CU properly exempt permitted persons from CTR filing by filing a "Designation of Exempt Person" form? (1020.315)		
10.0.e	For exempt persons, does the CU perform an annual review of the account (1020.315) to ensure the exemption remains appropriate? Is this review documented?		
11.0.0	Does the CU have an adequate Customer Due Diligence (CDD) process for identifying suspicious transactions and monitoring accounts for suspicious activity? (1020.320(a)(2)(iii))		
11.0.a	Is a Suspicious Activity Report (SAR) filed within 30 calendar days from the date of the initial detection of facts that may constitute a basis for filing a SAR? (1020.320(b)(3))		
11.0.b	Is supporting documentation for a SAR retained for 5 years? (1020.320(d))		
11.0.c	Does CU document decision process on whether to file a non-mandatory SAR?		
11.0.d	Does the CU complete SARs fully, accurately and in accordance with form instructions?		
11.0.e	Is the Board of Directors promptly notified of all SARs filed? (748.1(c)(4))		
Recordkeeping			
12.0.0	Does the CU maintain the necessary information for the purchase or issuance, by currency, of credit union checks, cashier's checks, traveler's checks, and money orders for amounts between $3,000 and $10,000? (1010.415(a)) and (1010.415(b))		
13.0.0	Does the CU maintain adequate historical records on the following transactions for 5 years:		
13.0.a	Extensions of credit greater than $10,000, except those secured by an interest in real property? (1010.410(a))		
13.0.b	Attempts to transfer more than $10,000 to or from any person, account or place outside the U.S.? (1010.410(b))		
13.0.c	All signature cards? (1020.410(b)(1))		
13.0.d	Member transaction statements or ledger cards? (1020.410(b)(2))		
13.0.e	CU and member share drafts or money orders over $100? (1020.410(b)(3))		
13.0.f	All withdrawals, other than share drafts or money orders, over $100 to accounts, except CU charges or periodic charges made pursuant to an agreement? (1020.410(b)(4))		
13.0.g	Transfers of more than $10,000 to any person, account, or place outside the US? (1020.410(b)(5,6))		

		Yes/No/NA	Comments
13.0.h	Drafts over $10,000 issued by, or drawn on, a foreign bank and paid by the CU? (1020.410(b)(7))		
13.0.i	Transfers of credit, cash, drafts, other checks, investment securities or other monetary instruments over $10,000 received directly from a foreign bank, broker or dealer in currency located outside the US? (1020.410(b)(8,9))		
13.0.j	Records which allow tracing of deposited share drafts over $100? (1020.410(b)(10))		
13.0.k	Name, address, taxpayer ID#, date of transaction, description of instrument, and method of payment for purchases and redemptions of share certificates? (1020.410(b)(11,12))		
13.0.l	Deposit slips or credit checks for transactions, or equivalent wire transfer and direct deposit transactions, over $100 which specify the amount of currency involved? (1020.410(b)(13))		
Specific Products & Services			
14.0.0	Since the prior exam, has the CU originated or received any wire transfers?		
14.0.a	With regard to wire transfers, does the CU retain, for 5 years, the required information for each payment order that it accepts of $3,000 or more? (1010.410(e))		
14.0.b	Is the required wire transfer information, identified in the above question, retrievable by reference to the originator's name and account number? (1010.410(e)(4))		
15.0.0	Since the prior exam, has the CU been involved with the transportation of currency outside the US or maintenance of an account in a foreign country?		
15.0.a	Does the CU file FINCEN Form 105 for the physical transportation of currency in excess of $10,000 into or outside the USA? (1010.340)		
15.0.b	Is a Report of Foreign Bank and Financial Accounts indicating a financial interest in an account in a foreign county filed annual on or before June 30? (1010.350)		
Information Sharing			
16.0.0	Has the CU designated accurate point of contact information on the CU Online program to receive 314(a) information requests from FinCEN regarding investigations of terrorist activity or money laundering? (1020.520(b)(2)(iii))		
16.0.a	Is the CU accessing the electronic list on FinCEN's secure website? (1020.520(b))		
16.0.b	Does the CU begin its search, required by the 314a information request, promptly and complete it within 2 weeks, reporting any matches to FinCEN upon detection? (1020.520(b)(2))		
17.0.0	Does the CU voluntarily share 314b information with other financial institutions for purposes of identifying and reporting suspected terrorist activity or money laundering? (1020.540)		
17.0.a	Has the CU submitted a Section 314(b) notice to FinCEN for the current year? (1020.540(b)(2))		
17.0.b	Has the CU verified that its information sharing partner completed the 314(b) notice? (1020.540(b)(3))		
Third Party Service Providers			
18.0.0	Is the CU using a third party service provider?		

		Yes/No/NA	Comments
18.0.a	Does the CU have an adequate due diligence process for reviewing actions taken by the third party to comply with BSA requirements on behalf of the CU?		
MSB-Money Services Businesses			
19.0.0	Does the credit union provide account services to money services businesses (MSBs)?		
19.0.a	Is the credit union correctly reporting MSB accounts on the quarterly 5300 Call Report per the Call Report Instructions?		
20.0.0	Does the credit union have adequate policies, procedures, and processes to identify and assess the risk related to MSB accounts?		
21.0.0	Has the credit union established policies, procedures and processes consistent with the interagency guidance released on April 26, 2005 for accounts opened or maintained for money services businesses (MSBs) to:		
21.0.a	Apply the CU's Customer Identification Program (CIP) procedures?		
21.0.b	Confirm FinCEN registration, if required? Note: Registration must be renewed every two years.		
21.0.c	Confirm state licensing, if applicable?		
21.0.d	Conduct a risk assessment to determine the level of risk associated with each MSB account and whether further due diligence is required?		
22.0.0	Is the credit union's system for monitoring MSB accounts for suspicious activities, and for reporting of suspicious activities, adequate?		
23.0.0	Are the credit union's overall policies, procedures, and processes associated with the MSB accounts adequate to reasonably protect the credit union from money laundering and terrorist financing?		
23.0.a	Are internal controls appropriate for the complexity of the institution and the risk posed by the MSB accounts?		
23.0.b	Do results of testing indicate the credit union's risk assessment of its MSB accounts is appropriate?		
24.0.0	Does the credit union exempt any MSBs from CTR filing?		
25.0.0	Has the credit union verified that less than 50% of the exempted entity's gross revenues are related to MSB related services?		
Testing Internal Controls			
26.0.0	Test the CU's internal control function by reviewing a minimum of 10 account level transactions for BSA compliance	*When responding "Yes" for testing, briefly describe tests in comment section.*	
26.0.a	Were transactions reviewed for compliance with Basic Requirements - Practice (Q6-8)		
26.0.b	Were transactions reviewed for compliance with Reporting Requirements (Q10-11)		
26.0.c	Were transactions reviewed for compliance with Recordkeeping Requirements (Q12-13)		
26.0.d	Were transactions reviewed for compliance with Specific Product and Service requirements? (Q14-15)		
26.0.e	Were transactions reviewed for compliance with Information Sharing Requirements (Q16-17)		
26.0.f	Enter the total number of transactions tested.		
Conclusion			
27.0.0	Did the examination identify required CTR or SAR forms that were not filed?		
20.0.a	For the required CTR forms that were not filed, will the credit union seek a CTR backfiling determination?		

		Yes/No/NA	Comments
28.0.0	Based on the results of exam testing, are the CU's internal controls effective?		
28.0.a	Are internal controls appropriate for the complexity of the institution?		
28.0.b	Do results of testing indicate credit union's risk assessment is appropriate?		

Customer Due Diligence — Overview

Objective. *Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).*

The cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers, particularly those that present a higher risk for money laundering and terrorist financing. The objective of CDD is to enable the bank to understand the nature and purpose of customer relationships, which may include understanding the types of transactions in which a customer is likely to engage. These processes assist the bank in determining when transactions are potentially suspicious.

Effective CDD policies, procedures, and processes provide the critical framework that enables the bank to comply with regulatory requirements including monitoring for and reporting of suspicious activity. An illustration of this concept is provided in Appendix K ("Customer Risk versus Due Diligence and Suspicious Activity Monitoring"). CDD policies, procedures, and processes are critical to the bank because they can aid in:

- Detecting and reporting unusual or suspicious activity that potentially exposes the bank to financial loss, increased expenses, or other risks.
- Avoiding criminal exposure from persons who use or attempt to use the bank's products and services for illicit purposes.
- Adhering to safe and sound banking practices.

Customer Due Diligence

FinCEN's final rule on CDD became effective July 11, 2016, with a compliance date of May 11, 2018. The rule codifies existing supervisory expectations and practices related to regulatory requirements and therefore, nothing in this final rule is intended to lower, reduce, or limit the due diligence expectations of the federal functional regulators or in any way limit their existing regulatory discretion.[1]

In accordance with regulatory requirements, all banks must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence,[2] including, but not limited to:

- Obtaining and analyzing sufficient customer information to understand the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and
- Conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information

[1] Department of the Treasury, Financial Crimes Enforcement Network (2016), "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29403.
[2] See 31 CFR 1020.210(b)(5)

regarding the beneficial owner(s) of legal entity customers. Additional guidance can be found in the examination procedures "Beneficial Ownership Requirements for Legal Entity Customers."

At a minimum, the bank must establish risk-based CDD procedures that:

- Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the bank to conduct ongoing monitoring
  - for the purpose of identifying and reporting suspicious transactions and,
  - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition, the bank's risk-based CDD policies, procedures, and processes should:

- Be commensurate with the bank's BSA/AML risk profile, with increased focus on higher risk customers.
- Contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Customer Risk Profile

The bank should have an understanding of the money laundering and terrorist financing risks of its customers, referred to in the rule as the customer risk profile.[3] This concept is also commonly referred to as the customer risk rating. Any customer account may be used for illicit purposes, including money laundering or terrorist financing. Further, a spectrum of risks may be identifiable even within the same category of customers. The bank's program for determining customer risk profiles should be sufficiently detailed to distinguish between significant variations in the money laundering and terrorist financing risks of its customers. Improper identification and assessment of a customer's risk can have a cascading effect, creating deficiencies in multiple areas of internal controls and resulting in an overall weakened BSA compliance program.

The assessment of customer risk factors is bank-specific, and a conclusion regarding the customer risk profile should be based on a consideration of all pertinent customer information, including ownership information generally. Similar to the bank's overall risk assessment, there are no required risk profile categories and the number and detail of these categorizations will vary based on the bank's size and complexity. Any one single indicator is not necessarily determinative of the existence of a lower or higher customer risk.

[3] See 31 CFR 1020.210(b)(5)(i)

Examiners should primarily focus on whether the bank has effective processes to develop customer risk profiles as part of the overall CDD program. Examiners may review individual customer risk decisions as a means to test the effectiveness of the process and CDD program. In those instances where the bank has an established and effective customer risk decision-making process, and has followed existing policies, procedures, and processes, the bank should not be criticized for individual customer risk decisions unless it impacts the effectiveness of the overall CDD program, or is accompanied by evidence of bad faith or other aggravating factors.

The bank should gather sufficient information about the customer to form an understanding of the nature and purpose of customer relationships at the time of account opening. This understanding may be based on assessments of individual customers or on categories of customers. An understanding based on "categories of customers" means that for certain lower-risk customers, the bank's understanding of the nature and purpose of a customer relationship can be developed by inherent or self-evident information such as the type of customer, the type of account opened, or the service or product offered.

The factors the bank should consider when assessing a customer risk profile are substantially similar to the risk categories considered when determining the bank's overall risk profile. The bank should identify the specific risks of the customer or category of customers, and then conduct an analysis of all pertinent information in order to develop the customer's risk profile. In determining a customer's risk profile, the bank should consider risk categories, such as the following, as they relate to the customer relationship:

- Products and Services.
- Customers and Entities.
- Geographic Locations.

As with the risk assessment, the bank may determine that some factors should be weighted more heavily than others. For example, certain products and services used by the customer, the type of customer's business, or the geographic location where the customer does business, may pose a higher risk of money laundering or terrorist financing. Also, actual or anticipated activity in a customer's account can be a key factor in determining the customer risk profile. Refer to the further description of identification and analysis of specific risk categories in the "BSA/AML Risk Assessment - Overview" section of the FFIEC BSA/AML Examination Manual.

Customer Information – Risk-Based Procedures

As described above, the bank is required to form an understanding of the nature and purpose of the customer relationship. The bank may demonstrate its understanding of the customer relationship through gathering and analyzing information that substantiates the nature and purpose of the account. Customer information collected under CDD requirements for the purpose of developing a customer risk profile and ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, includes beneficial ownership information for legal entity customers. However, the collection of customer information regarding beneficial ownership is governed by the

requirements specified in the beneficial ownership rule. The beneficial ownership rule requires the bank to collect beneficial ownership information at the 25 percent ownership threshold regardless of the customer's risk profile. In addition, the beneficial ownership rule does not require the bank to collect information regarding ownership or control for certain customers that are exempted or not included in the definition of legal entity customer, such as certain trusts, or certain other legal entity customers.[4]

Other than required beneficial ownership information, the level and type of customer information should be commensurate with the customer's risk profile, therefore the bank should obtain more customer information for those customers that have a higher customer risk profile and may find that less information for customers with a lower customer risk profile is sufficient. Additionally, the type of appropriate customer information will generally vary depending on the customer risk profile and other factors, for example, whether the customer is a legal entity or an individual. For lower risk customers, the bank may have an inherent understanding of the nature and purpose of the customer relationship (*i.e.*, the customer risk profile) based upon information collected at account opening. As a result, the bank may not need to collect any additional customer information for these customers in order to comply with this part of the CDD requirements.

Customer information collected under the CDD rule may be relevant to other regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties. The bank should define in its policies, procedures and processes how customer information will be used to meet other regulatory requirements. For example, the bank is expected to use the customer information and customer risk profile in its suspicious activity monitoring process to understand the types of transactions a particular customer would normally be expected to engage in as a baseline against which suspicious transactions are identified and to satisfy other regulatory requirements.[5]

The bank may choose to implement CDD policies, procedures, and processes on an enterprise-wide basis. To the extent permitted by law, this implementation may include sharing or obtaining customer information across business lines, separate legal entities within an enterprise, and affiliated support units. To encourage cost effectiveness, enhance efficiency, and increase availability of potentially relevant information, the bank may find it useful to cross-check for customer information in data systems maintained within the financial institution for other purposes, such as credit underwriting, marketing, or fraud detection.

Higher Risk Profile Customers

Customers that pose higher money laundering or terrorist financing risks, (*i.e.*, higher risk profile customers), present increased risk exposure to banks. As a result, due diligence policies, procedures, and processes should define both when and what additional customer information will be collected based on the customer risk profile and the specific risks posed. Collecting additional information about customers that pose heightened risk, referred to as enhanced due diligence (EDD), for example, in the private and foreign correspondent banking context, is part

[4] See 31 CFR 1010.230(e)(2) and 31 CFR 1010.230(h)
[5] See 31 CFR 1020.210(b)(5)(ii)

of an effective due diligence program. Even within categories of customers with a higher risk profile, there can be a spectrum of risks and the extent to which additional ongoing due diligence measures are necessary may vary on a case-by-case basis. Based on the customer risk profile, the bank may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship, such as:

- Source of funds and wealth.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).
- Financial statements for business customers.
- Location where the business customer is organized and where they maintain their principal place of business.
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the business customer's primary trade area, whether transactions are expected to be domestic or international, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.

Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions in order to assist the bank in determining when transactions are potentially suspicious. This determination is necessary for a suspicious activity monitoring system that helps to mitigate the bank's compliance and money laundering risks.

Consistent with the risk-based approach, the bank should do more in circumstances of heightened risk, as well as to mitigate risks generally. Information provided by higher risk profile customers and their transactions should be reviewed more closely at account opening and more frequently throughout the term of their relationship with the bank. The bank should establish policies and procedures for determining whether and/or when, on the basis of risk, obtaining and reviewing additional customer information, for example through negative media search programs, would be appropriate.

While not inclusive, certain customer types, such as those found in the "Persons and Entities" section of the FFIEC BSA/AML Examination Manual, may pose heightened risk. In addition, existing laws and regulations may impose, and supervisory guidance may explain expectations for, specific customer due diligence and, in some cases, enhanced due diligence requirements for certain accounts or customers, including foreign correspondent accounts,[6] payable-through

[6] See 31 CFR 1010.610.

accounts,[7] private banking accounts,[8] politically exposed persons,[9] and money services businesses.[10] The bank's risk-based customer due diligence and enhanced due diligence procedures must ensure compliance with these existing requirements and should meet these supervisory expectations.

Ongoing Monitoring of the Customer Relationship

The requirement for ongoing monitoring of the customer relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Therefore, in addition to policies, procedures, and processes for monitoring to identify and report suspicious transactions, the bank's CDD program must include risk-based procedures for performing ongoing monitoring of the customer relationship, on a risk basis, to maintain and update customer information, including beneficial ownership information of legal entity customers.[11] For more information on beneficial ownership of legal entity customers, refer to the "Beneficial Ownership Requirements for Legal Entity Customers" section of the FFIEC BSA/AML Examination Manual.

The requirement to update customer information is event-driven and occurs as a result of normal monitoring.[12] Should the bank become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information accordingly. Additionally, if this customer information is material and relevant to assessing the risk of a customer relationship, then the bank should reassess the customer risk profile/rating and follow established bank policies, procedures, and processes for maintaining or changing the customer risk profile/rating. One common indication of a material change in the customer risk profile is transactions or other activity that are inconsistent with the bank's understanding of the nature and purpose of the customer relationship or with the customer risk profile.

The bank's procedures should establish criteria for when and by whom customer relationships will be reviewed, including updating customer information and reassessing the customer's risk profile. The procedures should indicate who in the organization is authorized to change a customer's risk profile. A number of factors may be relevant in determining when it is appropriate to review a customer relationship including, but not limited to:

- Significant and unexplained changes in account activity
- Changes in employment or business operation

[7] See 31 CFR 1010.610(b)(1)(iii).
[8] See 31 CFR 1010.620
[9] Department of State, Department of the Treasury, Federal Reserve, FDIC, OCC, OTS, *Guidance on Enhanced Scrutiny for Transactions that may Involve the Proceeds of Official Corruption*, January 1, 2001.
[10] FinCEN, Federal Reserve, FDIC, NCUA, OCC, OTS, *Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States,* April 26, 2005.
[11] See 31 CFR 1020.210(b)(5)(ii)
[12] Department of the Treasury, Financial Crimes Enforcement Network (2016), "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29399.

- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring
- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

The ongoing monitoring element does not impose a categorical requirement that the bank must update customer information on a continuous or periodic basis. [13] However, the bank may establish policies, procedures, and processes for determining whether and when, on the basis of risk, periodic reviews to update customer information should be conducted to ensure that customer information is current and accurate.

[13] Ibid.

Examination Procedures

Customer Due Diligence

Objective. *Assess the bank's compliance with the regulatory requirements for customer due diligence (CDD).*

1. Determine whether the bank has developed and implemented appropriate written risk-based procedures for conducting ongoing CDD and that they:

- Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the bank to conduct ongoing monitoring
  - for the purpose of identifying and reporting suspicious transactions and,
  - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.
- Enable the bank to use customer information and the customer risk profile to understand the types of transactions a particular customer would be expected to engage in and as a baseline against which suspicious transactions are identified.

2. Determine whether the bank, as part of the overall CDD program, has effective processes to develop customer risk profiles that identify the specific risks of individual customers or categories of customers.

3. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank's BSA/AML risk profile with increased focus on higher risk customers.

4. Determine whether policies, procedures, and processes contain a clear statement of management's and staff's responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer's risk profile, as applicable.

5. Determine that the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering or terrorist financing that include whether and/or when, on the basis of risk, it is appropriate to obtain and review additional customer information.

6. Determine whether the bank provides guidance for documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

7. Determine whether the bank has defined in its policies, procedures, and processes how customer information, including beneficial ownership information for legal entity customers, is used to meet other relevant regulatory requirements, including but not limited to, identifying suspicious activity, identifying nominal and beneficial owners of private banking accounts, and determining OFAC sanctioned parties.

Transaction Testing

8. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of customer information. Determine whether the bank collects appropriate information sufficient to understand the nature and purpose of the customer relationship and effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. This sample can be performed when testing the bank's compliance with its policies, procedures, and processes as well as when reviewing transactions or accounts for possible suspicious activity.

9. On the basis of examination procedures completed, including transaction testing, form a conclusion about the adequacy of policies, procedures, and processes associated with CDD.

Beneficial Ownership Requirements for Legal Entity Customers – Overview

Objective. *Assess the bank's written procedures and overall compliance with regulatory requirements for identifying and verifying beneficial owner(s) of legal entity customers.*

Under the Beneficial Ownership Rule,[1] a bank must establish and maintain written procedures that are reasonably designed to identify and verify beneficial owner(s) of legal entity customers and to include such procedures in its anti-money laundering compliance program.

Legal entities, whether domestic or foreign, can be used to facilitate money laundering and other crimes because their true ownership can be concealed. The collection of beneficial ownership information by banks about legal entity customers can provide law enforcement with key details about suspected criminals who use legal entity structures to conceal their illicit activity and assets. Requiring legal entity customers seeking access to banks to disclose identifying information, such as the name, date of birth, and Social Security number of natural persons who own or control them will make such entities more transparent, and thus less attractive to criminals and those who assist them.

Similar to other customer information that a bank may gather, beneficial ownership information collected under the rule may be relevant to other regulatory requirements. These other regulatory requirements include, but are not limited to, identifying suspicious activity, and determining Office of Foreign Assets Control (OFAC) sanctioned parties. Banks should define in their policies, procedures, and processes how beneficial ownership information will be used to meet other regulatory requirements.

Legal Entity Customers

For the purposes of the Beneficial Ownership Rule,[2] a legal entity customer is defined as a corporation, limited liability company, or other entity that is created by the filing of a public document with a Secretary of State or other similar office, a general partnership, and any similar entity formed under the laws of a foreign jurisdiction that opens an account. A number of types of business entities are excluded from the definition of legal entity customer under the Beneficial Ownership rule. In addition, and subject to certain limitations, banks are not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens certain types of accounts. For further information on exclusions and exemptions to the Beneficial Ownership Rule, see Appendix 1. These exclusions and exemptions do not alter or supersede other existing requirements related to BSA/AML and OFAC sanctions.

Beneficial Owner(s)

Beneficial ownership is determined under both a control prong and an ownership prong. Under the control prong, the beneficial owner is a single individual with significant

[1] See 31 CFR 1010.230
[2] See 31 CFR 1010.230(e)(1)

responsibility to control, manage or direct a legal entity customer.[3] This includes, an executive officer or senior manager (Chief Executive Officer, Chief Financial Officer, Chief Operating Officer, President), or any other individual who regularly performs similar functions. One beneficial owner must be identified under the control prong for each legal entity customer.

Under the ownership prong, a beneficial owner is 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.[4] If a trust owns directly or indirectly, through any contract, arrangement, understanding, relationship or otherwise, 25 percent or more of the equity interests of a legal entity customer, the beneficial owner is the trustee.[5] Identification of a beneficial owner under the ownership prong is *not required* if no individual owns 25 percent or more of a legal entity customer. Therefore, all legal entity customers will have a total of between one and five beneficial owner(s) – one individual under the control prong and zero to four individuals under the ownership prong.

Banks may rely on the information supplied by the legal entity customer regarding the identity of its beneficial owner or owners, provided that it has no knowledge of facts that would reasonably call into question the reliability of such information.[6] However, bank staff who know, suspect, or have reason to suspect that equity holders are attempting to avoid the reporting threshold may, depending on the circumstances, be required to file a SAR.[7] More information on filing of SARs may be found in the "Suspicious Activity Reporting Overview" section on page 60 of the *FFIEC BSA/AML Examination Manual*.

Identification of Beneficial Ownership Information

A bank must establish and maintain written procedures detailing the identifying information that must be obtained for each beneficial owner of a legal entity customer opening a new account after May 11, 2018. At a minimum, the bank must obtain the following identifying information for each beneficial owner of a legal entity customer:

- Name.
- Date of birth.
- Address.[8]

[3] See 31 CFR 1010.230(d)(2)
[4] See 31 CFR 1010.230(d)(1)
[5] See 31 CFR 1010.230(d)(3)
[6] See 31 CFR 1010.230(b)(2)
[7] Department of the Treasury, Financial Crimes Enforcement Network (2016), "Customer Due Diligence Requirements for Financial Institutions," final rules (RIN 1506-AB25), *Federal Register*, vol. 81 (May 11), p. 29410.
[8] For an individual: a residential or business street address, or if the individual does not have such an address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, the residential or business street address of next of kin or of another contact individual, or a description of the customer's physical location. For a person other than an individual (such as a corporation, partnership, or trust): a principal place of business, local office, or other physical location. See 31 CFR 1010.220(a)(2)(i)(3)

- Identification number.[9]

A bank may obtain identifying information for beneficial owner(s) of legal entity customers through a completed certification form[10] from the individual opening the account on behalf of the legal entity customer, or by obtaining from the individual the information required by the form by another means, provided the individual certifies, to the best of the individual's knowledge, the accuracy of the information. A bank may rely on the information supplied by the individual opening the account on behalf of the legal entity customer regarding the identity of its beneficial owner(s), provided that it has no knowledge of facts that would reasonably call into question the reliability of such information. If a legal entity customer opens multiple accounts a bank may rely on the pre-existing beneficial ownership records it maintains, provided that the bank confirms (verbally or in writing) that such information is up-to-date and accurate at the time each account is opened.[11]

Banks must have procedures to maintain and update customer information, including beneficial ownership information for legal entity customers, on the basis of risk. Additionally, banks are not required to conduct retroactive reviews to obtain beneficial ownership information on legal entity customers that were existing customers as of May 11, 2018. However, the bank may need to obtain (and thereafter update) beneficial ownership information for existing legal entity customers based on its ongoing monitoring. For further guidance on maintaining and updating of customer information including beneficial ownership information, please see the "Ongoing Monitoring of Customer Relationship" section of the "Customer Due Diligence Overview" section of the *FFIEC BSA/AML Examination Manual*.[12]

Verification of Beneficial Owner Information

A bank must establish and maintain written risk-based procedures for verifying the identity of each beneficial owner of a legal entity customer within a reasonable period of time after the account is opened. These procedures must contain the elements required for verifying the identity of customers that are individuals under 31 CFR 1020.220(a)(2), provided, that in the case of documentary verification, the bank may use photocopies or other reproductions of the documents listed in paragraph (a)(2)(ii)(A)(*1*) of 31 CFR 1020.220. Guidance on documentary and non-documentary verification methods may be found in the core overview section "Customer Identification Program," of the *FFIEC BSA/AML Examination Manual*.

[9] An identification number for a U.S. person is a taxpayer identification number (TIN) (or evidence of an application for one), and an identification number for a non-U.S. person is one or more of the following: a TIN; a passport number and country of issuance; an alien identification card number; or a number and country of issuance of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard. TIN is defined by section 6109 of the Internal Revenue Code of 1986 (26 USC 6109) and the IRS regulations implementing that section (e.g., Social Security number (SSN) or individual taxpayer identification number (ITIN), or employer identification number (EIN)). See 31 CFR 1010.220(a)(2)(i)(4)

[10] See 31 CFR 1010.230, Appendix A, *Certification Regarding Beneficial Owners of Legal Entity Customers* (2016)

[11] FinCEN, FIN-2018-G001, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions*, Question #10, April 2018.

[12] FFIEC, *Core Examination Overview and Procedures, Customer Due Diligence Overview*, May 2018.

A bank need not establish the accuracy of every element of identifying information obtained, but must verify enough information to form a reasonable belief that it knows the true identity of the beneficial owner(s) of the legal entity customer. The bank's procedures for verifying the identity of the beneficial owners must describe when it uses documents, non-documentary methods, or a combination of methods.

Lack of Identification and Verification of Beneficial Ownership Information

Also consistent with 31 CFR 1020.220, the bank should establish policies, procedures, and processes for circumstances in which the bank cannot form a reasonable belief that it knows the true identity of the beneficial owner(s) of a legal entity customer. These policies, procedures, and processes should describe:

- Circumstances in which the bank should not open an account.
- The terms under which a customer may use an account while the bank attempts to verify the identity of the beneficial owner(s) of a legal entity customer.
- When the bank should close an account, after attempts to verify the identity of the beneficial owner(s) of a legal entity customer have failed.
- When the bank should file a SAR in accordance with applicable law and regulation.

Recordkeeping and Retention Requirements

A bank must establish recordkeeping procedures for beneficial ownership identification and verification information. At a minimum, the bank must maintain any identifying information obtained, including without limitation the certification (if obtained), for a period of five years after the date the account is closed.

The bank must also keep a description of any document relied on (noting the type, any identification number, place of issuance and, if any, date of issuance and expiration), of any non-documentary methods and the results of any measures undertaken, and of the resolution of each substantive discrepancy for five years after the record is made.

Reliance on Another Financial Institution

A bank is permitted to rely on the performance by another financial institution (including an affiliate) of the requirements of the Beneficial Ownership Rule with respect to any legal entity customer of the covered financial institution that is opening, or has opened, an account or has established a similar business relationship with the other financial institution to engage in services, dealings, or other financial transactions, provided that:

- Reliance is reasonable, under the circumstances.
- The relied-upon financial institution is subject to a rule implementing 31 USC 5318(h) and is regulated by a federal functional regulator.[13]

[13] Federal functional regulator means: Federal Reserve, FDIC, NCUA, OCC, U.S. Securities and Exchange Commission (SEC), or U.S. Commodity Futures Trading Commission (CFTC).

- The other financial institution enters into a contract requiring it to certify annually to the bank that it has implemented its AML program, and that it will perform (or its agent will perform) the specified requirements of the bank's procedures to comply with the requirements of the Beneficial Ownership Rule.

Examination Procedures

Beneficial Ownership

Objective: *Assess the bank's written procedures and overall compliance with regulatory requirements for identifying and verifying beneficial owner(s) of legal entity customers.*

1. Determine whether the bank has adequate written procedures for gathering and verifying information required to be obtained, and retained (including name, address, taxpayer identification number (TIN), and date of birth) for beneficial owner(s) of legal entity customers who open an account after May 11, 2018.

2. Determine whether the bank has adequate risk-based procedures for updating customer information, including beneficial owner information, and maintaining current customer information.

Transaction Testing

3. On the basis of a risk assessment, prior examination reports, and a review of the bank's audit findings, select a sample of new accounts opened for legal entity customers since May 11, 2018 to review for compliance with the Beneficial Ownership Rule. The sample should include a cross-section of account types. From this sample, determine whether the bank has performed the following procedures:

- Opened the account in accordance with the requirements of the Beneficial Ownership Rule (31 CFR 1010.230).
- Obtained the identifying information for each beneficial owner of a legal entity customer as required (e.g. name, date of birth, address, and identification number).
- Within a reasonable time after account opening, verified enough of the beneficial owner's identity information to form a reasonable belief as to the beneficial owner's true identity.
- Appropriately resolved situations in which beneficial owner's identity could not be reasonably established.
- Maintained a record of the identity information required by the Beneficial Ownership Rule, the method used to verify identity, and verification results (31 CFR 1010.230(i)).
- Filed SARs as appropriate.

4. On the basis of the examination procedures completed, including transaction testing, form a conclusion about the adequacy of procedures for complying with the Beneficial Ownership Rule

Appendix 1 – Beneficial Ownership

Exclusions from the definition of Legal Entity Customer

Under 31 CFR 1010.230(e)(2) a legal entity customer does not include:

- A financial institution regulated by a federal functional regulator[14] or a bank regulated by a state bank regulator;
- A person described in 31 CFR 1020.315(b)(2) through (5):
  - A department or agency of the United States, of any state, or of any political subdivision of any State;
  - Any entity established under the laws of the United States, of any state, or of any political subdivision of any state, or under an interstate compact between two or more states, that exercises governmental authority on behalf of the United States or any such state or political subdivision;
  - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York Stock Exchange or the American Stock Exchange (currently known as the NYSE American) or have been designated as a NASDAQ National Market Security listed on the NASDAQ stock exchange (with some exceptions);
  - Any subsidiary (other than a bank) of any "listed entity" that is organized under the laws of the United States or of any state and at least 51 percent of whose common stock or analogous equity interest is owned by the listed entity, provided that a person that is a financial institution, other than a bank, is an exempt person only to the extent of its domestic operations;
- An issuer of a class of securities registered under section 12 of the Securities Exchange Act of 1934 or that is required to file reports under section 15(d) of that Act;
- An investment company, investment adviser, an exchange or clearing agency, or any other entity that is registered with the SEC;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant that is registered with the CFTC;
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act;
- A bank holding company or savings and loan holding company;
- A pooled investment vehicle that is operated or advised by a financial institution that is excluded under paragraph (e)(2);
- An insurance company that is regulated by a state;

[14] Federal functional regulator means: Federal Reserve, FDIC, NCUA, OCC, U.S. Securities and Exchange Commission (SEC), or U.S. Commodity Futures Trading Commission (CFTC).

- A financial market utility designated by the Financial Stability Oversight Council;
- A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
- A non-U.S. governmental department, agency, or political subdivision that engages only in governmental rather than commercial activities;
- Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620.

Trusts

Trusts are not included in the definition of legal entity customer, other than statutory trusts created by a filing with a Secretary of State or similar office.[15]

Exemptions from the Ownership Prong

Certain legal entity customers are subject only to the control prong of the beneficial ownership requirement, including:

- A pooled investment vehicle operated or advised by a financial institution not excluded under paragraph 31 CFR 1010.230(e)(2); and
- Any legal entity that is established as a nonprofit corporation or similar entity and has filed its organizational documents with the appropriate state authority as necessary.

Exemptions and Limitations on Exemptions

Subject to certain limitations, banks are not required to identify and verify the identity of the beneficial owner(s) of a legal entity customer when the customer opens any of the following categories of accounts:

- Accounts established at the point-of-sale to provide credit products, including commercial private label credit cards, solely for the purchase of retail goods and/or services at these retailers, up to a limit of $50,000;
- Accounts established to finance the purchase of postage and for which payments are remitted directly by the financial institution to the provider of the postage products;
- Accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker;
- Accounts established to finance the purchase or leasing of equipment and for which payments are remitted directly by the financial institution to the vendor or lessor of this equipment.

These exemptions will not apply:

- If the accounts are transaction accounts through which a legal entity customer can

[15] FinCEN, FIN-2016-G003, *Frequently Asked Questions Regarding Customer Due Diligence Requirements for Financial Institutions*, Question #22, July 19, 2016.

make payments to, or receive payments from, third parties.

- If there is the possibility of a cash refund on the account activity opened to finance the purchase of postage, to finance insurance premiums, or to finance the purchase or leasing of equipment, then beneficial ownership of the legal entity customer must be identified and verified by the bank as required either at the initial remittance, or at the time such refund occurs.