TO THE OFFICER IN CHARGE OF SUPERVISION AND APPROPRIATE SUPERVISORY AND EXAMINATION STAFF AT EACH FEDERAL RESERVE BANK AND BANKING ORGANIZATIONS SUPERVISED BY THE FEDERAL RESERVE


Applicability: This letter is relevant to banking organizations supervised by the Federal Reserve that are subject to the Bank Secrecy Act.

Members of the Federal Financial Institutions Examination Council (FFIEC) released a new section and updated three sections with related examination procedures to the Bank Secrecy Act/Anti-Money Laundering (BSA/AML) Examination Manual. The Manual provides instructions to examiners when assessing the adequacy of a bank’s BSA/AML compliance program, relative to its risk profile, and the bank’s compliance with BSA regulatory requirements. These sections provide further transparency into the BSA/AML examination process and do not establish new requirements. The FFIEC drafted and revised the sections in close collaboration with the U.S. Treasury Department’s Financial Crimes Enforcement Network (FinCEN). The sections included in this release are:

- Introduction – Customers (New Section)
- Charities and Nonprofit Organizations
- Independent Automated Teller Machine Owners or Operators
- Politically Exposed Persons

These sections provide information and considerations related to certain customers that may indicate the need for bank policies, procedures, and processes to address potential money laundering, terrorist financing, and other illicit financial activity risks. The updates are based on concepts conveyed in the previously issued Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons and the Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit

---

1 Five of the six FFIEC member agencies develop and release the BSA/AML Examination Manual: the Federal Reserve Board (Federal Reserve), Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and State Liaison Committee (agencies). The Consumer Financial Protection Bureau is also a voting member of the FFIEC.

Organizations. These interagency statements make clear that no specific customer type automatically presents a higher money laundering, terrorist financing risk. They further state that banks that operate in compliance with applicable BSA/AML requirements and reasonably manage and mitigate risks related to the unique characteristics of the customer relationship are neither prohibited nor discouraged from providing banking services to any specific class or type of customer.

The revisions to the Manual continue to emphasize the agencies’ risk-focused approach to BSA/AML supervision and reinforce the distinction between regulatory requirements and considerations set forth in guidance. Further, the revisions incorporate regulatory requirements and other changes, as applicable.

Revised sections of the Manual are attached and will be identified by a 2021 date on the FFIEC BSA/AML InfoBase. The agencies will continue to review and revise the remaining sections of the 2014 edition of the Manual and release updates as they are completed. Previous updates include those from April 2020, February 2021, and June 2021. All Manual updates are catalogued on the FFIEC BSA/AML InfoBase under the “What’s New” page.


Reserve Banks are asked to distribute this letter to the supervised banking organizations in their districts and to appropriate supervisory staff. Questions regarding this letter may be sent via the Board’s public website.

Michael S. Gibson
Director
Division of Supervision and Regulation

Attachments:
- Introduction - Customers
- Charities and Nonprofit Organizations
- Independent Automated Teller Machine Owners or Operators

---

3 Federal Reserve, FDIC, FinCEN, NCUA, OCC (November 19, 2020), “Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations.”
• Politically Exposed Persons

Supersedes:

INTRODUCTION - CUSTOMERS

The subsections within Risks Associated with Money Laundering and Terrorist Financing (ML/TF) provide information and considerations that may indicate the need for bank policies, procedures, and processes to address potential ML/TF and other illicit financial activity risks related to certain products, services, customers, and geographic locations. Not all of the examination and testing procedures included in the Risks Associated with Money Laundering and Terrorist Financing sections will apply to every bank, or be used during every examination.

Examiners are reminded that no specific customer type automatically presents a higher risk of ML/TF or other illicit financial activity. Further, banks that operate in compliance with applicable Bank Secrecy Act/anti-money laundering (BSA/AML) regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to any specific class or type of customer.

Customer relationships present varying levels of ML/TF and other illicit financial activity risks, and the potential risk to a bank depends on the presence or absence of numerous factors. Not all customers pose the same risk, and not all customers of a particular type are automatically higher risk. The potential risk to a bank depends on the facts and circumstances specific to the customer relationship. The federal banking agencies and FinCEN, encourage banks to manage customer relationships and mitigate risks based on those customer relationships rather than declining to provide banking services to entire categories of customers.

The following sections on different customer types are intended to be a subset of a broader review of compliance with BSA/AML regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting. However, there is no BSA/AML regulatory requirement or supervisory expectation for banks to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer. Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship.

Banks must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop customer risk profiles. The information collected to create a customer risk profile should also assist banks in conducting

---

1 “Joint Statement on the Risk-Focused Approach to BSA/AML Supervision,” issued by the Board of Governors of the Federal Reserve System (Federal Reserve), the Federal Deposit Insurance Corporation (FDIC), the Financial Crimes Enforcement Network (FinCEN), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC), July 22, 2019.

2 12 CFR 208.63(b)(2); 12 CFR 211.244(j); 12 CFR 326.8(b)(2); 12 CFR 748.2(b)(2); 12 CFR 21.21(c)(2); 31 CFR 1020.220.


4 31 CFR 1010.230.

5 12 CFR 208.62; 211.5(k); 211.244(f); and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(e) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).

6 There may be supervisory expectations for other reasons, such as safety and soundness standards, corporate governance, bank-specific enforcement actions and conditions for obtaining bank charters and deposit insurance.

ongoing monitoring to identify and report any suspicious activity. Examiners should assess how a bank evaluates customers according to their particular characteristics to determine whether the bank can effectively mitigate the risk customers may pose.

The scoping and planning process will help examiners to focus their reviews of risk management practices and compliance with BSA/AML regulatory requirements on areas with the greatest ML/TF and other illicit financial activity risk, which may include some customer types or groups. The specific examination procedures performed will depend on factors such as the bank’s risk profile, size, or complexity, expansionary activities, adoption of new innovations or technologies, changes to the bank’s BSA/AML compliance officer or department, the quality of the bank’s independent testing, and other relevant factors. As appropriate, examiners will assess whether the bank has developed and implemented adequate policies, procedures, and processes to identify, measure, monitor, and control risks customers may pose, and to otherwise comply with related BSA/AML regulatory requirements.
CHARITIES AND NONPROFIT ORGANIZATIONS

Objective: Evaluate the bank’s policies, procedures, and processes to assess, manage, and mitigate potential risks associated with customers that are charities and other nonprofit organizations (NPOs). Evaluate the bank’s compliance with regulatory requirements such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to customers that are charities and other NPOs.

Many charities and other nonprofit organizations (NPOs) pursue activities that are intended to serve the public good and provide various services, including building communities, relieving suffering, providing life-saving assistance, and helping developing nations. The federal banking agencies and FinCEN have recognized that it is vital for legitimate charities and other NPOs to have access to financial services, including the ability to transmit funds in a timely manner.¹

Examiners are reminded that no specific customer type automatically presents a higher risk of money laundering, terrorist financing (ML/TF), or other illicit financial activity. Further, banks that operate in compliance with applicable Bank Secrecy Act/anti-money laundering (BSA/AML) regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to charities and other NPOs.

Risk Factors

Charity and other NPO customers present varying levels of ML/TF and other illicit financial activity risks, and the potential risk to a bank depends on the presence or absence of numerous factors. Examiners are reminded that the U.S. government does not view the charitable sector as a whole as presenting a uniform or unacceptably high risk of being used or exploited for ML/TF or sanctions violations.² The potential risk to the bank depends on the facts and circumstances specific to the customer relationship, such as transaction volume, type of activity, and geographic locations.

The ML/TF risk for charity and other NPO customers can also vary depending on the operations, activities, leadership, and affiliations of the organization. For example, U.S. charities that operate and provide funds solely to domestic recipients generally present lower ML/TF risk. However, those U.S. charities that operate abroad, or that provide funding to, or have affiliated organizations in conflict regions can face potentially higher ML/TF risks.³

¹ See “Joint Fact Sheet on Bank Secrecy Act Due Diligence Requirements for Charities and Non-Profit Organizations” issued by the federal banking agencies (Federal Reserve, FDIC, NCUA, OCC) and FinCEN.
³ Id.
Risk Mitigation

Understanding a customer’s risk profile enables the bank to apply appropriate policies, procedures, and processes to manage and mitigate risk and otherwise comply with BSA/AML regulatory requirements. Like all bank accounts, those held by charity and other NPO customers are subject to BSA/AML regulatory requirements. These include requirements related to customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting. However, there is no BSA/AML regulatory requirement or supervisory expectation for banks to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer. Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship.

Banks must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop customer risk profiles. Examiners should assess how a bank evaluates charity and other NPO customers according to their particular characteristics to determine whether the bank can effectively mitigate the risk these customers may pose. Consistent with a risk-based approach for conducting ongoing CDD, a bank should typically obtain more customer information for those customers with a higher customer risk profile and may collect less information for customers with a lower customer risk profile, as appropriate.

The information collected to create a customer risk profile should also assist banks in conducting ongoing monitoring to identify and report any suspicious activity. Moreover, performing an appropriate level of ongoing CDD that is commensurate with the customer’s risk profile assists the bank in determining whether a customer’s transactions are suspicious.

Charities and other NPOs are also subject to federal and state reporting requirements and regulatory oversight. For example, charities report specific information annually on IRS Form 990 regarding their stated mission, programs, finances (including non-cash contributions), donors, activities, and funds sent and used abroad. Many NPOs also

---

4 For more information about customer risk profiles, see the Customer Due Diligence section.
5 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(i)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); 12 CFR 748.2(b)(2) (NCUA); 12 CFR 21.21(c)(2) (OCC); and 31 CFR 1020.220 (FinCEN).
7 31 CFR 1010.230 and 1010.230(e)(3)(ii). Charity and NPO customers are subject only to the control prong of the beneficial ownership requirement.
8 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).
9 There may be supervisory expectations for other reasons, such as safety and soundness standards, corporate governance, bank-specific enforcement actions and conditions for obtaining bank charters and deposit insurance.
11 The extensive Schedule F of Form 990 includes many categories of reporting requirements for charities with overseas activities.
adhere to voluntary self-regulatory standards and controls to improve individual governance, management, and operational practice, in addition to internal controls required by donors and others.

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. The following information may be useful for a bank in understanding the nature and purpose of the customer relationship and in determining the ML/TF and other illicit financial activity risk profile of charity and other NPO customers:

- Purpose and nature of the charity and NPO, including mission(s), stated objectives, programs, activities, and services.
- Organizational structure, including key principals and management.
- Geographic locations served, including headquarters and operational areas, particularly in higher-risk areas where terrorist groups are most active.
- Information pertaining to the operating policies, procedures, and internal controls of the charity and NPO.
- State incorporation or registration, and tax-exempt status by the Internal Revenue Service (IRS) and required reports with regulatory authorities.
- Voluntary participation in self-regulatory programs to enhance governance, management, and operational practice.
- Financial statements, audits, and any self-assessment evaluations.
- General information about the donor base, funding sources, and fundraising methods, and, for public charities, the level of support from the general public.
- General information about beneficiaries and criteria for disbursement of funds, including guidelines/standards for qualifying beneficiaries and any intermediaries that may be involved.
- Affiliation with other charities and NPOs, governments, or groups.

Additional information that may be useful in determining the customer risk profile of a charity or other NPO is available at the U.S. Department of the Treasury’s Resource Center, Protecting Charitable Organizations. Refer to the Customer Due Diligence and Suspicious Activity Reporting sections for more information.

Examiner Evaluation

Examiners should evaluate the bank’s processes for assessing risks associated with

---

customers that are charities and NPOs. Examiners should determine whether the bank’s internal controls are designed to ensure ongoing compliance and are commensurate with the bank’s risk profile. Examiners should also determine whether internal controls manage and mitigate ML/TF and other illicit financial activity risks for charity and other NPO customers. Examiners may conduct this assessment when evaluating the bank’s compliance with regulatory requirements, such as customer identification, CDD, and suspicious activity reporting. More information can be found in the *Assessing the BSA/AML Compliance Program - BSA/AML Internal Controls* and *Assessing Compliance with BSA Regulatory Requirements* sections of this Manual.
CHARITIES AND NONPROFIT ORGANIZATIONS
EXAMINATION AND TESTING PROCEDURES

Objective: Evaluate the bank’s policies, procedures, and processes to assess, manage, and mitigate risks associated with customers that are charities and other nonprofit organizations (NPOs). Evaluate the bank’s compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting, with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to customers who are charities and other NPOs.

The following examination and testing procedures are intended to be a subset of a broader review of compliance with Bank Secrecy Act/anti-money laundering (BSA/AML) regulations, such as customer identification, customer due diligence (CDD), beneficial ownership, and suspicious activity reporting. Not all of the examination and testing procedures will apply to every bank or will be used during every examination.

1. Determine whether the bank has developed and implemented appropriate, written risk-based procedures for conducting ongoing CDD for all customers, including charity and other nonprofit organization (NPO) customers, and that these procedures enable the bank to:
   - Understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
   - 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. (As a reminder, charity and NPO customers are only subject to the control prong of the beneficial ownership requirement, which requires the identification and verification of a single individual with significant responsibility to control, manage, or direct a legal entity customer.)
   - Use customer information and the customer risk profile to understand the types of transactions in which a particular customer would be expected to engage, and to establish 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 including, as appropriate, charity and other NPO customers.

3. Determine whether the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering, terrorist financing (ML/TF), and other illicit financial activities, which may include certain charities and other NPOs. Policies, procedures, and processes generally include whether and when, based on risk, it is appropriate to obtain and review additional customer
information, including guidance for resolving issues when insufficient, inaccurate, or unverifiable information is obtained. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank’s ML/TF and other illicit financial activity risk profile.

4. Determine whether the bank’s system for monitoring charity and other NPO customer accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank’s risk profile.

5. Determine if performing risk-focused testing is appropriate based on the review of a risk assessment, prior examination reports, other examination information, or a review of the bank’s audit findings. If risk-focused testing is appropriate, select a sample of charity and other NPO customer relationships and request applicable documentation to perform risk-focused testing. From the sample selected, perform the following examination procedures:

- Determine whether the bank collects appropriate information to understand the nature and purpose of customer relationships and to evaluate such customers according to their particular characteristics when assessing whether the bank can effectively mitigate the potential risk those customers may pose.

- Determine whether the bank effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile. (As a reminder, charity and NPO customers are only subject to the control prong of the beneficial ownership requirement, which requires the identification and verification of a single individual with significant responsibility to control, manage, or direct a legal entity customer.)

- Review transaction activity for selected customer relationships and, if necessary, request and review specific transactions and transaction monitoring documentation to determine whether the bank has identified and reported any suspicious activity.

6. Based on examination and testing procedures completed, form a conclusion about the adequacy of, and the bank’s adherence to, its policies, procedures, and processes associated with charity and other NPO customers.
INDEPENDENT AUTOMATED TELLER MACHINE OWNERS OR OPERATORS

Objective: Evaluate the bank’s policies, procedures, and processes to assess, manage, and mitigate potential risks associated with customers who are independent automated teller machine (ATM) owners or operators, including Independent Sales Organizations (ISOs). Evaluate the bank’s compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, currency transaction reporting, and suspicious activity reporting with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to customers who are independent ATM owners or operators, including ISOs.

Automated Teller Machines (ATMs) offer fast and convenient access to cash and are an important channel in providing financial services, including in underserved markets. Independent ATMs are ATMs not owned by banks. An independent ATM operator is a person or an entity that is in the business of owning, leasing, managing, or otherwise controlling access to the interior of an ATM, including its internal cash vault. The independent ATM operator may be the same or different from the independent ATM owner. Independent ATMs may be found in a wide variety of public and retail venues.

There are various business models that may apply to bank customers who own or operate independent ATMs. For some bank customers, independent ATM ownership or operation is their core business. For others, it is an ancillary service offered as a convenience to their customers. A retail business, for example, may purchase or lease an independent ATM to better serve its cash customers, attract new customers to its business, or add revenue to its primary retail business through service fees charged to customers who use the independent ATM.

Where independent ATM ownership or operation is the customer’s core business, a company may own and deploy multiple ATMs that service thousands of consumers. Many operators of these independent ATMs are also considered Independent Sales Organizations (ISOs). An ISO is generally a person or entity that is (1) approved by, and under contract with, a sponsor bank to deploy and service independent ATMs and (2) under contract with an approved acquiring processor to route independent ATM transactions to Electronic Funds Transfer (EFT) networks for which the ISO has been registered by the sponsor bank.

---

1 This section focuses on independent ATMs that offer remote access to customer accounts for the purpose of making balance inquiries or cash withdrawals. The agencies recognize that financial services kiosks that allow individuals to facilitate payments or other types of transactions, or to purchase or sell convertible virtual currencies, are sometimes referred to as ATMs. These latter entities may be engaged in money transmission consistent with FinCEN guidance. See FinCEN (May 9, 2019), FIN-2019-G001, “Application of FinCEN’s Regulation to Certain Business Models Involving Convertible Virtual Currencies.” These ATMs may present additional or different risks, and the agencies may provide additional guidance to examiners in this area.

2 A sponsor bank is a financial institution that is a member of one or more electronic funds transfer networks having a program to allow registration of ISOs for authorized access by ATMs to such networks.
EFT networks include national (e.g., Visa’s PLUS and MasterCard’s CIRRUS) and regional networks (e.g., NYCE and STAR). ISOs are contractually subject to the EFT network’s rules, and if the ISO also provides network access to other independent ATM owners or operators, it also has a responsibility to ensure that these independent ATM owners or operators comply with the EFT network’s requirements. In practice, agreements between the independent ATM owner or operator and the ISO reflect the establishment of all management and operating policies relating to the ISO’s acquiring processor and for the independent ATM owner or operator in complying with the standards of the EFT network.

For all types of independent ATMs, owners or operators generally need bank accounts to supply cash for the ATMs and to settle the electronic funds transfers used to process the ATM transactions. The owner or operator may elect to replenish cash in the ATM and conduct other basic maintenance, or the ISO may complete these functions.

Examiners are reminded that no specific customer type automatically presents a higher risk of money laundering, terrorist financing (ML/TF), or other illicit financial activity. Further, banks that operate in compliance with applicable Bank Secrecy Act/anti-money laundering (BSA/AML) regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to independent ATM owner or operator customers, including those that are ISOs.

**Risk Factors**

Independent ATM owner or operator customers present varying levels of ML/TF and other illicit financial activity risks, and the potential risk to a bank depends on the presence or absence of numerous factors. Not all independent ATM owner or operator customers pose the same risk, and not all independent ATM owner or operator customers are automatically higher risk. The potential risk to a bank depends on the facts and circumstances specific to the customer relationship, such as transaction volume, locations of the ATMs, and the source of funds to replenish the ATMs.

Because of the cash-intensive nature of an ATM, the source of funds used to replenish the ATM is a key risk factor. Independent ATM owners or operators that fund their ATM replenishment solely with cash withdrawn from their account at a bank pose a relatively lower ML/TF risk because the bank knows the source of funds and can compare the volume of cash usage to EFT settlements to identify suspicious activity. Conversely, independent ATM owners or operators that replenish ATMs from other or unknown cash sources may present potentially higher ML/TF risks, as the source of cash can be difficult for the bank to verify.

ML/TF and other illicit financial activity may occur through independent ATMs when an ATM is replenished with illicit currency that is subsequently withdrawn by ATM users. Commingling cash from both illicit and legitimate sources in the ATM can make all transactions in the independent ATM owner’s or operator’s account appear to be legitimate. The independent ATM owner or operator would receive “clean” funds back via the ATM settlement process in the form of ACH deposits that appear to be from
legitimate sources but are actually part of an ML/TF or other illicit financial activity scheme.

Many states do not currently register, monitor the activity of, or examine independent ATM owners or operators. In addition, independent ATM owners or operators are not generally considered money services businesses and are, therefore, not required to have AML compliance programs. FinCEN concluded in 2007 that a nonbank owner/operator of an ATM that offers customers of a depository institution no service other than remote access to such customers’ accounts at those depository institutions for the purposes of making balance inquiries or currency withdrawals, would not be a money services business for purposes of the BSA and its implementing regulations. Therefore, an independent ATM owner or operator may not be separately regulated as a financial institution at the state or federal level.

Risk Mitigation

Understanding a customer’s risk profile enables the bank to apply appropriate policies, procedures, and processes to manage and mitigate risk, and comply with BSA/AML regulatory requirements. Like all bank accounts, those held by independent ATM owner or operator customers are subject to BSA/AML regulatory requirements. These include requirements related to customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, currency transaction reporting, and suspicious activity reporting. However, there is no BSA/AML regulatory requirement or supervisory expectation for banks to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer. Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship.

Banks must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships and to develop a customer risk profile. Examiners should assess how a bank evaluates independent ATM owner or operator customers according to their particular characteristics to determine whether the bank can effectively mitigate the risk these customers may pose. Consistent with a risk-based approach for conducting ongoing CDD, a bank should typically obtain more customer information for those customers with a higher customer risk profile and may

---

4 For more information about customer risk profile, see the Customer Due Diligence section.
5 12 CFR 208.63(b)(2), 211.5(m)(2), and 211.24(f)(2) (Federal Reserve); 12 CFR 326.8(b)(2) (FDIC); 12 CFR 748.2(b)(2) (NCUA); 12 CFR 21.21(c)(2) (OCC); and 31 CFR 1020.220 (FinCEN).
7 31 CFR 1010.230.
8 31 CFR 1020.310.
9 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).
10 There may be supervisory expectations for other reasons, such as safety and soundness standards, corporate governance, bank-specific enforcement actions and conditions for obtaining bank charters and deposit insurance.
collect less information for customers with a lower customer risk profile, as appropriate. Additional reviews and information collected by a sponsoring bank or ISO associated with determining compliance with EFT networks’ rules may also assist a bank in developing a customer risk profile.

The information collected to create a customer risk profile should also assist banks in conducting ongoing monitoring to identify and report suspicious activity. Moreover, performing an appropriate level of ongoing CDD commensurate with the customer’s risk profile assists the bank in determining whether a customer’s transactions are suspicious.

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. The following information may be useful for a bank in understanding the nature and purpose of the customer relationship, and therefore, in determining the ML/TF and other illicit financial activity risk profile of ISO or independent ATM owner or operator customers:

- Organizational structure, including key principals and management.
- Information pertaining to the operating policies, procedures, and internal controls of the ATM owner or operator.
- ATM currency servicing arrangements, contracts, and responsibilities (e.g., cash vault services, third-party providers, and self-service).
- Information regarding the source of funds if the bank account is not used to replenish the ATM. Sources of cash may include proceeds generated by the core retail business of the owner, proceeds from a loan or revolving credit line, or cash originating from an account maintained at another bank.
- Location where the independent ATM owner or operator customer is organized, and where they maintain their places of business, including locations of owned or operated ATMs.
- Description of expected and actual ATM activity levels, including currency transactions.
- Information to better understand whether ATM operations are generally ancillary to other retail operations or the primary business of the independent ATM owner or operator customer.

Risk may be reduced if all the operating accounts of an ISO, and the other independent ATM owners or operators to which the ISO provides network access, are with the same bank (the sponsor bank). In this case, the sponsor bank generally will have access to additional ISO and independent ATM owner or operator customer information collected at the time of sponsorship and information from the bank’s periodic audits and reviews of these sponsored entities.

Independent ATM owner or operator customers may use a separate bank account solely to fund ATM cash replenishment and receive automated clearing house transaction settlements. This account would be separate from other business activity and may reduce
risk by providing the bank with additional transparency into the flow and volume of funds associated with ATM operations.

Refer also to the Customer Due Diligence and Suspicious Activity Reporting sections for more information.

Examiner Evaluation

Examiners should evaluate the bank’s processes for assessing risks associated with customers that are independent ATM owners or operators. Examiners should determine whether the bank’s internal controls are designed to ensure ongoing compliance and are commensurate with the bank’s risk profile. Examiners should also determine whether internal controls manage and mitigate ML/TF and other illicit financial activity risks for independent ATM owner and operator customers. Examiners may conduct this assessment when evaluating the bank’s compliance with regulatory requirements, such as customer identification, CDD, and suspicious activity reporting. More information can be found in the Assessing the BSA/AML Compliance Program – BSA/AML Internal Controls and Assessing Compliance with BSA Regulatory Requirements sections of this Manual.
INDEPENDENT AUTOMATED TELLER MACHINE OWNERS OR OPERATORS EXAMINATION AND TESTING PROCEDURES

Objective: Evaluate the bank’s policies, procedures, and processes to assess, manage, and mitigate potential risks associated with independent automated teller machine (ATM) owner or operator customers, including Independent Sales Organizations (ISOs). Evaluate the bank’s compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, currency transaction reporting, and suspicious activity reporting, with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to independent ATM owner or operator customers, including ISOs.

The following examination and testing procedures are intended to be a subset of a broader review of compliance with Bank Secrecy Act/anti-money laundering (BSA/AML) regulations, such as customer identification, customer due diligence (CDD), beneficial ownership, currency transaction reporting, and suspicious activity reporting. Not all of the examination and testing procedures will apply to every bank or be used during every examination.

1. Determine whether the bank has developed and implemented appropriate, written risk-based procedures for conducting ongoing CDD for all customers, including independent automated teller machine (ATM) owner or operator customers, and that these procedures enable the bank to:
   - Understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
   - 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.
   - Use customer information and the customer risk profile to understand the types of transactions in which a particular customer would be expected to engage, and to establish 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 including, as appropriate, independent ATM owner or operator customers.

3. Determine whether the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering, terrorist financing (ML/TF), and other illicit financial activities, which may include independent ATM owner or operator customers. Policies, procedures, and processes generally include whether and when, based on risk, it is appropriate to obtain and review additional
customer information, including guidance for resolving issues when insufficient, inaccurate, or unverifiable information is obtained. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank’s ML/TF and other illicit financial activity risk profile.

4. Determine whether the bank’s system for monitoring independent ATM owner or operator customer accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank’s risk profile.

5. Consider whether the bank’s policies, procedures, and processes adequately address the preparation, filing, and retention of currency transaction reports for independent ATM owner or operator customers.

6. Determine if performing risk-focused testing is appropriate based on the review of a risk assessment, prior examination reports, other examination information, or a review of the bank’s audit findings. If risk-focused testing is appropriate, select a sample of independent ATM owner or operator customer relationships and request applicable documentation to perform risk-focused testing. From the sample selected, perform the following examination procedures:

- Determine whether the bank collects appropriate information to understand the nature and purpose of customer relationships, and to evaluate such customers according to their particular characteristics when assessing whether the bank can effectively mitigate the potential risk those customers may pose.
- Determine whether the bank effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile.
- Review transaction activity for selected customer relationships and, if necessary, request and review specific transactions and transaction monitoring documentation to determine whether the bank has identified and reported any suspicious activity.

7. Based on examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes associated with independent ATM owner or operator customers.
POLITICALLY EXPOSED PERSONS

Objective: Evaluate the bank’s policies, procedures, and processes to assess, manage, and mitigate potential risks associated with foreign individual customers who the bank has designated as politically exposed persons (PEPs). Evaluate the bank’s compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to foreign individual customers who the bank has designated as PEPs.

Bank Secrecy Act/Anti-Money Laundering (BSA/AML) regulations do not define the term Politically Exposed Person (PEP), and the term should not be confused with “senior foreign political figure” (SFPF), a subset of PEP. The term PEP is commonly used in the financial industry to refer to foreign individuals who are or have been entrusted with a prominent public function, as well as to their immediate family members and close associates.

Examiners are reminded that no specific customer type automatically presents a higher risk of money laundering, terrorist financing (ML/TF), or other illicit financial activity. Further, banks that operate in compliance with applicable BSA/AML regulatory requirements and reasonably manage and mitigate risks related to the unique characteristics of customer relationships are neither prohibited nor discouraged from providing banking services to foreign individuals who the bank may consider to be PEPs (referred to in this section as “bank-identified PEPs”).

Risk Factors

Bank-identified PEP customers present varying levels of ML/TF and other illicit financial activity risks, and the potential risk to a bank depends on the presence or absence of numerous factors. Not all bank-identified PEP customers pose the same risk, and not all bank-identified PEP customers are automatically higher risk. By virtue of their public position or relationships, some bank-identified PEPs may present a risk higher than other customers by having access to funds that may be the proceeds of corruption or other illicit activity. Some foreign individuals who are bank-identified PEPs have used banks as conduits for their illegal activities, including corruption, bribery, ML/TF, and other illicit financial activity. The potential risk to the bank depends on the facts and circumstances specific to the customer relationship, such as transaction volume, type of activity, and geographic locations.


2 31 CFR 1010.605(p) (Definitions) and 31 CFR 1010.620 (Due diligence programs for private banking accounts); see also “FinCEN Advisory on Human Rights Abuses Enabled by CORRUPT SENIOR FOREIGN POLITICAL FIGURES AND THEIR FINANCIAL FACILITATORS,” (June 2018). Specific to SFPFs, refer to the Private Banking Due Diligence Program (non-U.S. Persons) section for more information.

3 See “Joint Statement on Bank Secrecy Act Due Diligence Requirements for Customers Who May Be Considered Politically Exposed Persons,” issued by the federal banking agencies (Federal Reserve, FDIC, NCUA, OCC) and FinCEN.
Politically Exposed Persons

Bank-identified PEPs with a limited transaction volume, a low-dollar deposit account with the bank, known legitimate sources of funds, access only to products or services subject to specific terms and payment schedules, or a limited number of accounts with which the bank-identified PEP is associated, could reasonably be characterized as having lower customer risk profiles.

**Risk Mitigation**

Understanding a customer’s risk profile enables the bank to apply appropriate policies, procedures, and processes to manage and mitigate risk and comply with BSA/AML regulatory requirements. Like all bank accounts, those held by bank-identified PEPs or associated with bank-identified PEPs are subject to BSA/AML regulatory requirements. These requirements are related to customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting. However, there is no BSA/AML regulatory requirement or supervisory expectation for banks to have unique or additional customer identification requirements or CDD steps for any particular group or type of customer.

Consistent with a risk-based approach, the level and type of CDD should be commensurate with the risks presented by the customer relationship. The CDD rule does not require a bank to screen for or otherwise determine whether a customer or beneficial owner of a legal entity customer may be considered a PEP. A bank may choose to determine whether a customer is a PEP at account opening if the bank determines the information is necessary to develop a customer risk profile. Further, the bank may conduct periodic reviews with respect to bank-identified PEPs as part of, or in addition to, the required ongoing risk-based monitoring to maintain and update customer information.

Banks must have appropriate risk-based procedures for conducting ongoing CDD to understand the nature and purpose of customer relationships, and to develop a customer risk profile. Examiners should assess how a bank evaluates bank-identified PEP customers according to their particular characteristics to determine whether the bank can effectively mitigate the potential risk these customers may pose. Consistent with a risk-based approach for conducting ongoing CDD, a bank should typically obtain more customer information for those customers with a higher customer risk profile and may collect less information for customers with a lower customer risk profile, as appropriate.

The information collected to create a customer risk profile should also assist banks in conducting ongoing monitoring to identify and report suspicious activity. Moreover, performing an

---

4 For more information about customer risk profile, see the Customer Due Diligence section.
5 12 CFR 208.63(b)(2)211.5(m)(2)211.24(f)(2)12 CFR 326.8(b)(2)12 CFR 748.2(b)(2)12 CFR 21.21(c)(2)31 CFR 1020.220.
7 31 CFR 1010.230.
8 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR 1020.320 (FinCEN).
9 There may be supervisory expectations for other reasons, such as safety and soundness standards, corporate governance, bank-specific enforcement actions and conditions for obtaining bank charters and deposit insurance.
appropriate level of ongoing CDD commensurate with the customer’s risk profile assists the bank in determining whether a customer’s transactions are suspicious.

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. The following information may be useful for a bank in understanding the nature and purpose of the customer relationship and, therefore, in determining the ML/TF and other illicit financial activity risk profile of bank-identified PEP customers:

- The type of products and services used,\(^\text{11}\)  
- The volume and nature of transactions.  
- Geographies associated with the customer’s activity and domicile.  
- The customer’s official government responsibilities.  
- The level and nature of the customer’s authority or influence over government activities or officials.  
- The customer’s access to significant government assets or funds.

Banks may leverage existing processes for assessing geographically specific ML/TF, corruption, and other illicit financial activity risks when developing the customer risk profile. Existing processes may also take into account the jurisdiction’s legal and enforcement frameworks, including ethics reporting and oversight requirements. For a bank-identified PEP who is no longer in active government service, banks may also consider the time that the customer has been out of office and the level of influence he or she may still hold as factors in the customer risk profile.

When developing customer risk profiles and determining when to collect additional customer information, and what to collect, banks may take into account such factors as the customer’s public office or position of public trust (or that of the customer’s family members or close associates), as well as any indication that the bank-identified PEP misuses his or her authority or influence for personal gain.

Refer to the Customer Due Diligence and Suspicious Activity Reporting sections for more information.

**Examiner Evaluation**

Examiners should evaluate the bank’s processes for assessing risks associated with customers that are bank-identified PEPs. Examiners should determine whether the bank’s internal controls are designed to ensure ongoing compliance and are commensurate with the bank’s risk profile.

\(^\text{11}\) For example, some banks have wealth management accounts that fall outside of the definition of “private banking account” but may still pose a higher risk of illicit financial activity. These accounts are often held by high net worth individuals, and the accounts may contain large balances or be used for high dollar transactions. Banks are required to comply with BSA/AML regulatory requirements including, but not limited to, CDD and suspicious activity monitoring and reporting in relation to such wealth management accounts. Adherence to the existing BSA/AML framework will assist banks in identifying and managing the potentially higher risks associated with these customers and accounts.
Examiners should also determine whether internal controls manage and mitigate ML/TF and other illicit financial activity risks for bank-identified PEPs. Examiners may conduct this assessment when evaluating the bank’s compliance with regulatory requirements such as customer identification, CDD, and suspicious activity reporting. More information can be found in the *Assessing the BSA/AML Compliance Program - BSA/AML Internal Controls* and *Assessing Compliance with BSA Regulatory Requirements* sections of this Manual.
Politically Exposed Persons Examination and Testing Procedures

Objective: Evaluate the bank’s policies, procedures, and processes to assess, manage, and mitigate potential risks associated with foreign individual customers who the bank has designated as politically exposed persons (PEPs). Evaluate the bank’s compliance with regulatory requirements, such as customer identification, customer due diligence (CDD), beneficial ownership of legal entity customers, and suspicious activity reporting, with respect to these customers. Examiners are reminded that there are no Bank Secrecy Act (BSA) regulations specific to foreign individuals customers who the bank has designated as PEPs.

The following examination and testing procedures are intended to be a subset of a broader review of compliance with Bank Secrecy Act/anti-money laundering (BSA/AML) regulations, such as customer identification, customer due diligence (CDD), beneficial ownership, and suspicious activity reporting. Not all of the examination and testing procedures will apply to every bank or will be used during every examination.

1. Determine whether the bank has developed and implemented appropriate, written risk-based procedures for conducting ongoing CDD for all customers, including bank-identified PEP customers, and that these procedures enable the bank to:
   - Understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
   - 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.
   - Use customer information and the customer risk profile to understand the types of transactions in which a particular customer would be expected to engage, and to establish 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 including, as appropriate, bank-identified PEP customers.

3. Determine whether the bank has policies, procedures, and processes to identify customers that may pose higher risk for money laundering, terrorist financing (ML/TF), and other illicit financial activities, which may include bank-identified PEP customers. Policies, procedures, and processes generally include whether and when, based on risk, it is appropriate to obtain and review additional customer information, including guidance for resolving issues when insufficient, inaccurate, or unverifiable information is obtained. Determine whether the risk-based CDD policies, procedures, and processes are commensurate with the bank’s ML/TF and other illicit financial activity risk profile.
4. Determine whether the bank’s system for monitoring bank-identified PEP customer accounts for suspicious activities, and for reporting suspicious activities, is adequate given the bank’s risk profile.

5. Determine if performing risk-focused testing is appropriate based on the review of a risk assessment, prior examination reports, other examination information, or a review of the bank’s audit findings. If risk-focused testing is appropriate, select a sample of bank-identified PEP relationships and request applicable documentation to perform risk-focused testing. From the sample selected, perform the following examination procedures:

   - Determine whether the bank collects appropriate information to understand the nature and purpose of customer relationships, and to evaluate such customers according to their particular characteristics when assessing whether the bank can effectively mitigate the potential risk those customers may pose.

   - Determine whether the bank effectively incorporates customer information, including beneficial ownership information for legal entity customers, into the customer risk profile.

   - Review transaction activity for the selected customer relationships and, if necessary, request and review specific transactions and transaction monitoring documentation to determine whether the bank has identified and reported any suspicious activity.

6. Based on examination and testing procedures completed, form a conclusion about the adequacy of policies, procedures, and processes associated with bank-identified PEP customers.