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[1] 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[2] 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.[3] 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[4] 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,[5] customer due diligence (CDD),[6] beneficial ownership of legal entity customers,[7] currency transaction reporting,[8] and suspicious activity reporting.[9] However, there is no BSA/AML regulatory requirement or supervisory expectation[10] 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.[11] 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

[3] FinCEN (December 3, 2007), FIN-2007-G006 "Application of the Definition of Money Services Business to Certain Owner-Operators of Automated Teller Machines Offering Limited Services."
[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(j)(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).
[6] 31 CFR 1010.210 and 1020.210(a)(2)(v).
[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.
[11] 31 CFR 1020.210(a)(2)(v).

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.