Bank Secrecy and Anti-Money Laundering Act Newsletter

This newsletter is designed to provide a general education to agents and distributors about the Bank Secrecy Act (BSA) and Anti-Money Laundering (AML) requirements related to Netspend card programs and services. This newsletter should not be considered as legal, accounting, or tax advice.

As part of the BSA requirement, Netspend's AML program is in writing and includes:

1. Designated Compliance Officer
2. Established internal controls
3. Risk-based procedures to conduct ongoing customer due diligence
4. Ongoing training of Netspend employees, distributors, and agents
5. Independent review to test the program controls

YOUR RESPONSIBILITIES AS AN AGENT AND DISTRIBUTOR OF NETSPEND

As an agent/distributor of Netspend you are required to comply with BSA/AML requirements. Additionally, you have a responsibility to help detect and deter money laundering and terrorist financing activities in compliance with the BSA and other state and federal regulations. In order to assist you in complying with these requirements, Netspend strongly advises the following:

1. Implement an AML Program; this includes implementing Netspend's Risk and Compliance Guidelines.
2. Ensure all locations/stores offering Netspend products have a copy of Netspend's Risk and Compliance Guidelines readily available.

   Netspend provides its agents and distributors Risk and Compliance Guidelines as an extension of its AML Program. For your convenience, the Risk & Compliance Guidelines are always available at the following website designated for agents and distributors: https://www.netspend.com/compliance-guidelines/
3. Recognize the requirements of the Bank Secrecy Act (BSA).

   It mandates recordkeeping and reporting to help identify the source, volume, and movement of currency and other monetary instruments in or out of the United States and deposited into financial institutions.

   To accomplish its objective, the BSA requires financial institutions and some non-bank financial institutions (NBFIs), such as money service businesses (MSBs), to:

   a) Properly identify persons conducting transactions.
   b) File Suspicious Activity Reports (SARs).
      a. For transactions totaling $2,000.00 or more within 30 days from the date the suspicious transaction is detected.
   c) File Currency Transaction Reports (CTRs).
      a. For cash transactions totaling more than $10,000.00, conducted by a person in one day, within 15 calendar days from the date of the transaction.
   d) Maintain appropriate records of financial transactions for 5 years.

4. Know what Money Laundering is and identify the Three Stages of Money Laundering:

   a) **Stage 1: Placement:** The money launderer introduces the illegal proceeds into the financial system.
      Example: Place funds into circulation through financial institutions, casinos, and shops.
   b) **Stage 2: Layering:** The money launderer converts the proceeds of the crime into another form and creates layers of financial transactions to disguise the audit trail, source, and ownership of the funds.
      Example: Send wire transfers from one account to another account.
   c) **Stage 3: Integration:** The money launderer uses proceeds in normal transactions to create the perception of legitimacy. This stage provides the launderer the opportunity to increase his wealth with the proceeds of the crime.
      Example: Invests funds in real estate, financial ventures, or luxury assets.

5. Comprehend what the Customer Identification Program (CIP) requirements are and when to obtain/verify customer identity, as applicable.
6. Understand the purpose of the Office of Foreign Assets Control (OFAC).
    a) Enforces economic and trade sanctions against individuals, entities, and foreign governments with interests that are hostile to the United States.
    b) Publishes a list that identifies those parties with whom transactions are prohibited.

    OFAC rules require institutions and their employees to:

    a) Identify any property or transaction subject to economic sanctions.
    b) Block or reject the transaction.
    c) Freeze an account.
    d) Advise OFAC of the blocked asset or rejected transaction.
    e) Take actions as directed by OFAC.
    f) Release the blocked transaction or property only with OFAC's authorization.

    Failure to comply with OFAC regulations can lead to severe civil and criminal penalties, including jail time. Additional risks include:

    a) Charter forfeiture or loss of insured status.
    b) Monetary losses resulting from asset forfeiture actions and fines.
    c) Substantial legal fees.
    d) Reputational damage and negative publicity.
7. Actively recognize "red flags" and report suspicious activity, in addition to identifying suspicious activity through customer behavior and follow your store's procedures on how to handle.

    Potential Red Flags/Suspicious Customer Behavior

    a) Customer tries to provide an ID that is not theirs.
    b) Customer attempts to conduct transactions on multiple accounts.
    c) Customer declines to produce original documents for verification, when required.
    d) Customer asks questions about how to avoid reporting requirements.
    e) Customer threatens an employee to avoid reporting requirements.
    f) Customer abruptly withdraws a transaction.
    g) Customer refuses to proceed with a transaction, when additional information is requested.
    h) Customer requests to load funds when they are not present.

    Remain alert and report to Netspend any requests to load Netspend cards that are made by phone or email.

    a) All loads to Netspend cards must be performed in person, in exchange for cash/debit ONLY.
    b) Do not load any Netspend card over the phone, without the funds present.
    c) Netspend will **never** call you to load funds to a card as a 'test'.

IMPORTANT: The presence of a single 'red flag' is not, by itself, evidence of criminal activity; however, closer review of any red flag will help determine whether it is suspicious or not.

It is the responsibility of the agent, or distributor, to monitor financial transactions at their stores for any suspicious activity. If a customer demonstrates suspicious activity, you must:

Write Down the Details about the Activity

a) Who was suspicious? Was it a new customer, returning customer, etc.?
b) What was unusual about the transaction or the customer's behavior?
c) How was the card purchased or load made?
d) When and at what location did the activity occur?

Report Suspicious Activity to the Netspend Compliance Department

a) Complete the Unusual/Suspicious Activity Referral form: http://www.netspend.com/content/dam/netspend/compliance-guidelines/08_2024/DRF_Form.pdf

OR

b) Contact the Netspend Compliance Department at 1.866.914.7224 (p); 512.539.5839 (f); compliance@netspend.com

Do not inform the customer involved that any suspicious activity has been or will be reported to Netspend, or to FinCEN via a SAR report.

8. Understand Currency Transaction Report (CTR) requirements.

   A CTR is a form required to be completed by financial institutions under BSA to combat money laundering and other crimes.

   CTR Filing Requirements
   A CTR must be completed for each deposit, withdrawal, exchange of currency, or a physical transfer of currency of more than $10,000.00 conducted by, or on behalf of, one person, in a single day.

   a) **Currency** is coin and paper money of the United State, or any other country, which is circulated and customarily accepted as money.
   b) **Physical transfer of currency** does not include a transfer of funds by means of a bank check, bank draft, traveler's check, or wire transfer.

   Note: MSBs are required to complete CTRs.

   Currency Transaction Reporting & Suspicious Activity (SAR)
   If the CTR involves a currency transaction that is also suspicious, a SAR should be filed separately.

9. Fulfill recordkeeping requirements.
10. Meet state posting requirements.
11. Ensure employees are trained on these requirements on a regular basis.
12. Conduct an Independent Review of your AML Program to ensure you are complying with AML requirements.

Elder Abuse: Exploitation of Older Adults

The National Center on Elder Abuse (NCEA) defines elder abuse as the illegal or improper use of an older adult's funds, property or assets (i.e. financial exploitation). Financial exploitation is the most common form of elder abuse and only a small fraction of incidents are reported.

Detecting Elder Abuse
You may become aware of individuals conducting illicit activity or scams against the elderly through direct interactions with elderly customers who are being exploited. Branch or store personnel familiarity with specific victim customers may lead to the identification of unusual activity that initiates a review of the customer transactions. In addition, monitoring transaction activity that is inconsistent with the expected behavior may help you detect potential elder abuse.

Financial Crimes Enforcement Network (FinCEN) Guidelines on Elder Abuse
FinCEN provides a list of potential red flags that may be indicative of illicit activity against elders; these should be evaluated with other red flags and expected transaction activity conducted by or on behalf of the elder. Additional investigation and analysis may be necessary to determine whether the activity is suspicious. You play a key role in preventing elder financial abuse and have a duty to report suspected elder financial exploitation.

Red flag indicators for Elder Financial Exploitation:

Erratic or Unusual Purchases/Transactions or Changes in Account Patterns

a) Frequent large withdrawals, including daily maximum currency withdrawals from an ATM.
b) Sudden non-sufficient funds activity.
c) Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds.
d) Debit transactions that are inconsistent for the elder.
e) Uncharacteristic attempts to wire large sums of money.
f) Closing accounts without regard to penalties.

Interactions with Customers or Caregivers:

a) Caregiver or other individual shows excessive interest in the elder's finances or assets, does not allow the elder to speak for himself, or is reluctant to leave the elder's side during conversations.
b) Elder shows an unusual degree of fear or submissiveness toward the caregiver or expresses fear of eviction or nursing home placement, if the money is not given to a caretaker.
c) Financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her.
d) New caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation.
e) Elder moves away from existing relationships and toward new associations with other friends or strangers.
f) Elder's financial management changes suddenly, such as through a change of power of attorney or a different family member or individual.
g) Elder lacks knowledge about his or her financial status or shows a sudden reluctance to discuss financial matters.

If you suspect elder financial exploitation, REPORT IT IMMEDIATELY, to the following agencies:

a) Local law enforcement
b) Local Adult Protective Services (APS) www.eldercare.gov
c) FinCEN, via your internal SAR process, as applicable

Note: Your state may have additional reporting requirements.

Report Suspicious Activity and suspected elder financial exploitation to the Netspend Compliance Department

a) Complete the Unusual/Suspicious Activity Referral form: http://www.netspend.com/content/dam/netspend/compliance-guidelines/08_2024/DRF_Form.pdf

OR

b) Contact the Netspend Compliance Department at 1.866.914.7224 (p); 512.539.5839 (f); compliance@netspend.com

Do not inform the customer involved that any suspicious activity has been or will be reported to Netspend, or to FinCEN via a SAR report.

Contact Us

Please contact us at 1-866-397-5643 or partnersupport@netspend.com if any of the following apply:

- If you have had any changes to your business; for example, changes to your business name or changes in ownership.
- If you are no longer distributing, selling, or reloading Netspend products.
- If you have any questions or concerns regarding the distribution of Netspend cards.