Bank Secrecy Act (BSA) & Anti-Money Laundering (AML)

2024
Distributor Training

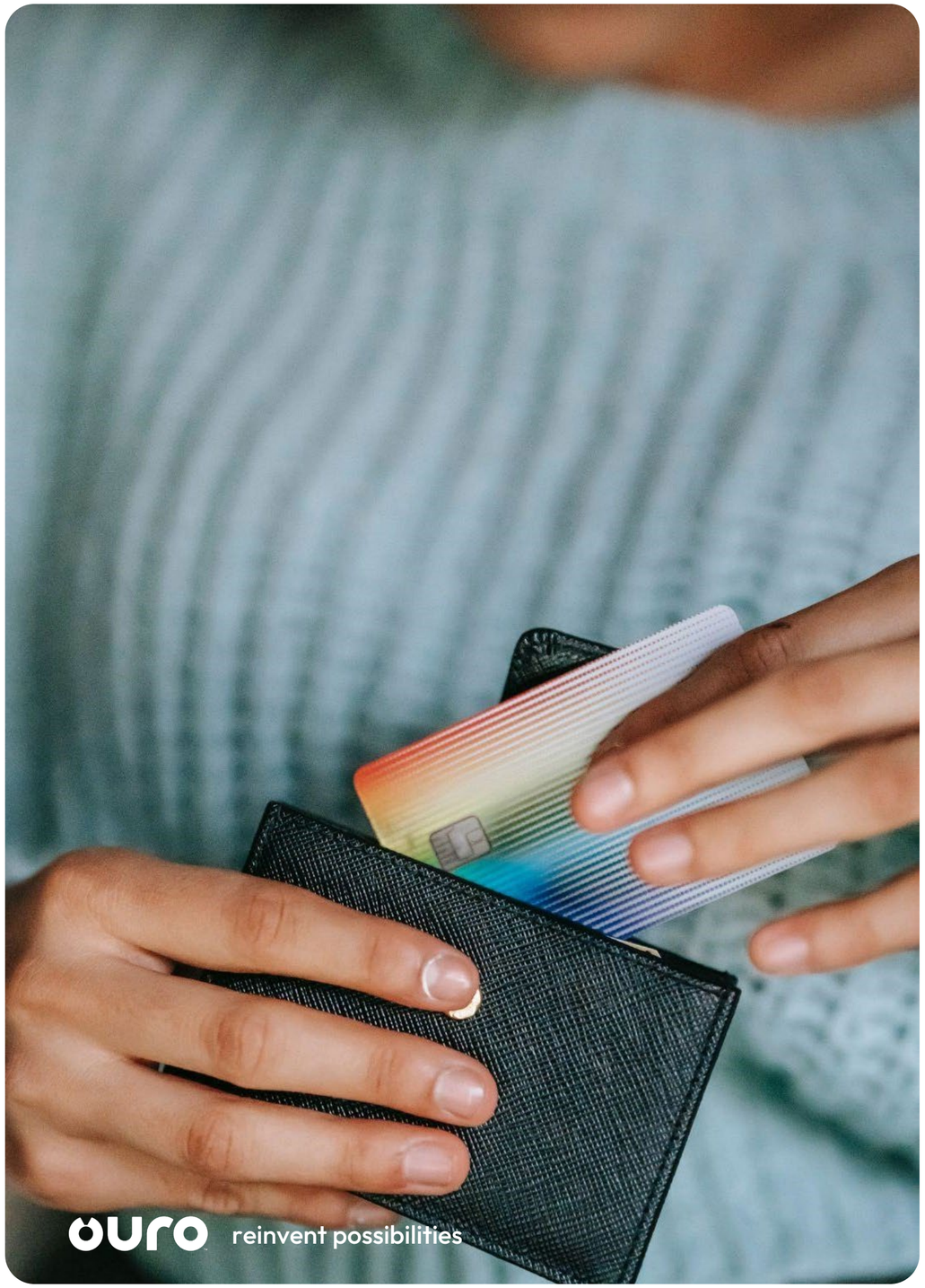
Legal Disclaimer: Ouro BSA/AML Training

- This training is designed to provide a general education to agents and distributors about detecting and preventing money laundering, terrorist financing, and other financial crimes related to Ouro card programs and services.
- This training is intended for general education purposes and nothing in this training should be considered to be legal, accounting, or tax advice.
- If you have specific questions of a legal, accounting, or tax nature that are related to this training, please consult your institution’s attorney, accountant, or tax professional.

What We Will Cover Today

After completing this training, you will be better prepared to:

- Understand your requirement to take this training
- Comply with state posting requirements
- Explain the background and purpose of the Bank Secrecy Act (BSA)
- Understand Customer Identification Program (CIP) requirements and when to obtain or verify customer identity
- Understand the purpose of the Office of Foreign Assets Control (OFAC) and penalties for noncompliance
- Understand basic money laundering and terrorist financing activity
- Recognize common “red flags” for money laundering
- Recognize common “red flags” for elder abuse
- Know when to report suspicious activity
- Understand the purpose of Currency Transaction Reports (CTRs)
- Provide guidance on what to do when a regulatory examiner visits your store



Bank Secrecy & Anti-Money Laundering Training

Objective: To ensure agents and distributors of Ouro card programs and services comply with the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) requirements and prevent Ouro products, programs, and services from being used to conduct or support illegal activities

Annual BSA/AML Training Requirement

As an agent and/or distributor of Ouro products and services, you are required to complete this ongoing training on BSA/AML requirements and must ensure your employees are trained on these requirements on a regular basis. You must maintain training documents and records confirming the completion of this training for at least 5 years from the original date of training.

Distributor Risk and Compliance Guidelines

As part of its AML Program, Ouro provides its agents and distributors Risk and Compliance Guidelines to implement at each location where Ouro products are distributed. The Risk and Compliance Guidelines and Ouro BSA/AML training materials are always available for review at the following website: https://www.netspend.com/compliance-guidelines

Important: As an agent and distributor of Ouro products, you are required to implement and maintain a current copy of the Risk and Compliance Guidelines at each location where Ouro products are distributed.

State Posting and Signage Requirements

Money Transmitter Signage At Retail Locations

Ouro has appointed you as its authorized agent to sell and reload Ouro products and services in those jurisdictions (subject states) where Ouro is licensed as a money transmitter. As an authorized agent of Ouro in the subject states, you may be engaged in the provision of money transmission services in connection with the sale and reload of Ouro products. Therefore, you are required to post such signs and/or other notifications by Ouro at all of your retail locations, as applicable.

The signage provided to you by Ouro must be conspicuously displayed so a customer with 20/20 vision is able to read it from the place where he or she would typically conduct business with you, or on a bulletin board, in plain view, on which you post notices to the general public.

It is your responsibility to ensure the signage is conspicuously posted in a timely manner at each of your retail locations. You may obtain a copy of your specific state signage here: https://www.netspend.com/compliance-guidelines

If you have any questions regarding the state posting requirements, please visit https://www.netspend.com/help/licenses or contact your account manager or Ouro Partner Services at 1.866.397.5643 or partnersupport@netspend.com.

Non-Bank Financial Institution (NBFI)

Non-Bank Financial Institutions are entities other than banks that offer financial services. Examples include:

- Money Service Businesses (MSBs), such as check cashing stores and money transmitters like Western Union or MoneyGram
- Casinos
- Insurance companies
- Pawnbrokers
- Loan or finance companies

Ouro is a non-bank financial institution, and you are a non-bank financial institution.

Some NBFIs, such as MSBs, are subject to the full range of BSA requirements as a bank institution to include:

- Customer Identification Program (CIP)
- Suspicious Activity Reporting (SAR)
- Currency Transaction Reporting (CTR)
- Recordkeeping requirements

You may work for an NBFI that **may or may not be** subject to these requirements; however, as an agent or distributor of Ouro products and services, you have a responsibility to help detect and deter money laundering and terrorist financing activities for compliance with the Bank Secrecy Act (BSA).

Failure to comply with BSA/AML regulations may lead to civil and criminal penalties, including jail time.

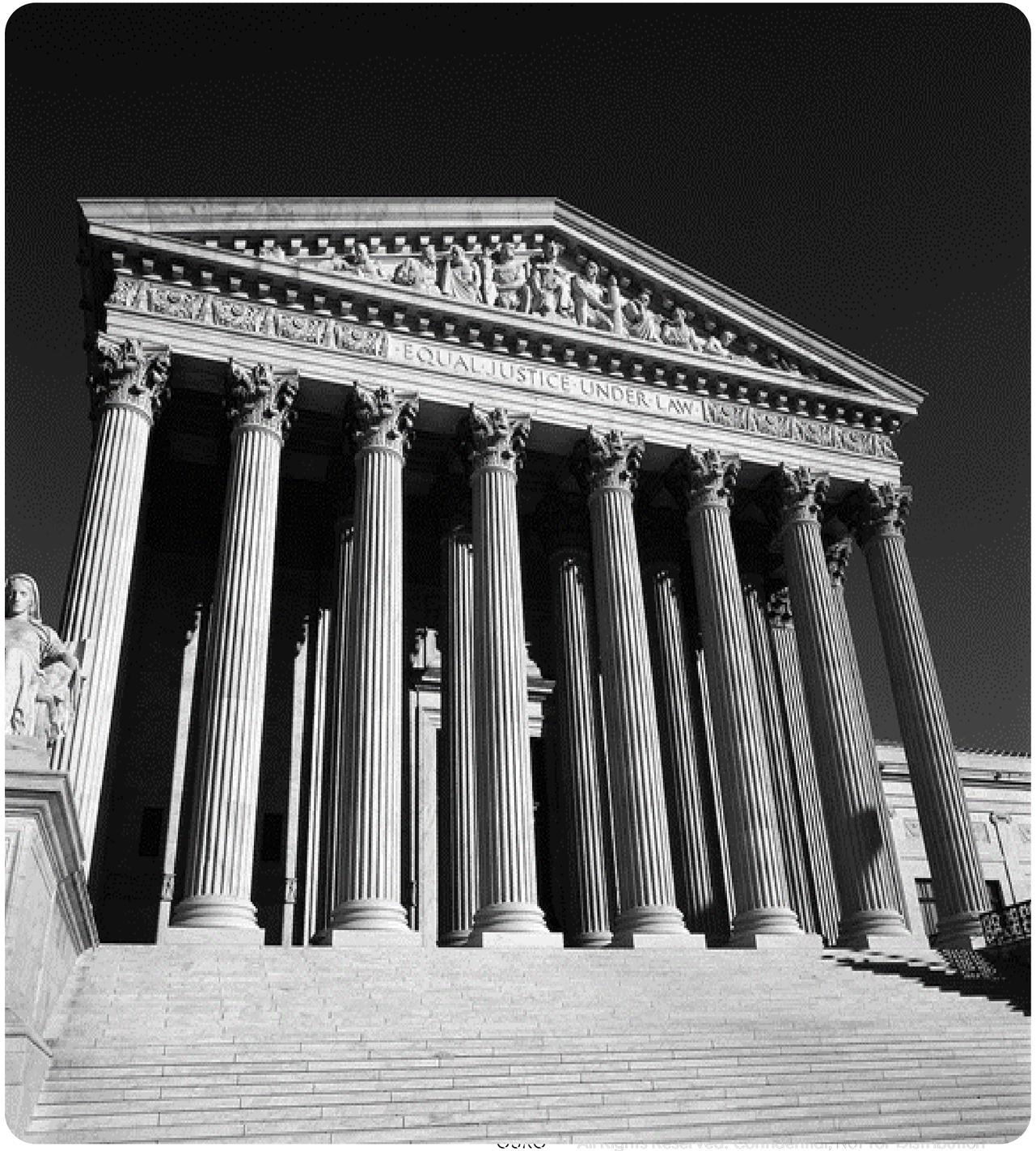
Bank Secrecy Act

The Bank Secrecy Act (BSA) assists law enforcement in investigating and prosecuting cases of money laundering, terrorist financing, and other financial crimes.

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:

- Formally establish and implement an anti-money laundering (AML) program
- Properly identify persons conducting transactions
- File Suspicious Activity Reports (SARs)
- For transactions totaling $2000.00 or more within 30 days from the date the suspicious transaction is detected
- File Currency Transaction Reports (CTRs)
- 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
- Maintain appropriate records of financial transactions for 5 years



Ouro’s Anti-Money Laundering (AML) Program

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

- Designated Compliance Officer
- Established internal controls
- Risk-based procedures to conduct ongoing customer due diligence
- Ongoing training of Ouro employees, distributors, and agents
- Independent review to test the program controls

BSA & Government Agencies

Government Agencies Responsible for Enforcement of BSA Regulations

The US Department of Treasury

The administrator of the BSA is the US Department of Treasury.

Federal Agencies

The federal agencies responsible for oversight of financial entities operating in the US with the authority to enforce BSA compliance include:

- Internal Revenue Service (IRS)
- Financial Crimes Enforcement Network (FinCEN)
- Consumer Financial Protection Bureau (CFPB)
- Federal Reserve Board (FRB)
- Office of the Comptroller of the Currency (OCC)
- National Credit Union Administration (NCUA)
- Federal Deposit Insurance Corporation (FDIC)

Financial Crimes Enforcement Network (FinCEN)

FinCEN issues regulations and interpretive guidance, supports the federal financial agency examination functions, and pursues enforcement actions.

BSA Statutes & Requirements

The Money Laundering Control Act 1980

Imposes criminal liabilities on financial institution that knowingly assist in money laundering activities

The Suspicious Activity Report (SAR) 1996

Requires financial institutions to report known or suspected criminal violations of federal law or suspicious transactions related to money laundering or BSA violations

The Annunzio-Wylie Anti-Money Laundering Act 1992

Strengthens the sanctions for BSA violations and the role of the US Treasury in combating money laundering

The USA PATRIOT Act 2001

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

Criminalizes the financing of terrorism and strengthens customer identification requirements

BSA: Customer Due Diligence (CDD) Requirements Final Rule 2016

Requires financial institutions to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions; effective July 11, 2016 for compliance by May 11, 2018

Customer Identification Program (CIP), Know Your Customer (KYC)

Under the USA PATRIOT Act, the US implemented the Customer Identification Program (CIP) requiring financial institutions to verify the identity of individuals using their services to conduct financial transactions. In addition, financial institutions must conduct a risk assessment of their customers and service offerings.

To Open An Account:

Ouro agents and distributors who operate in a non-retail environment, such as a check cashing store, must collect the following information from the customer:

- Legal name
- Date of birth
- Residential street address (P.O. Box is not allowed)
- Identification Number

Identification Number

For US citizens:

- Taxpayer identification number (TIN), such as a Social Security Number (SSN)

For non-US citizens, any of the following will suffice:

- Taxpayer identification number (TIN), such as a Social Security Number (SSN)
- Passport number and country of issuance
- Number and country of issuance of any government-issued photo ID

Note: If the customer has a foreign ID, you (or the customer) will need to send copies of the ID to Ouro.

Ouro will complete the CIP verification process and screen customers against high-risk databases and government sanctions lists.

ouro reinvent possibilities

Customer Identification Program (CIP) Recordkeeping

CIP Recordkeeping Requirements

Financial institutions must keep and maintain accurate and detailed records of the information collected and used to verify the individual's identity for a period of up to 5 years.

Penalties for Noncompliance

Financial institutions that do not follow these rules are subject to criminal and civil penalties.

Recordkeeping Requirements for Various States

Arizona, Oklahoma, and New Mexico have additional CIP recordkeeping requirements; these states require additional information for transactions of $1000.00 or more.

Required Identifying Information		
Arizona	**Oklahoma**	**New Mexico**
• The Legal Name of the Customer • Customer's Social Security Number or Taxpayer Identification Number, if any • Customer's ID Type and ID Number • Customer's current Occupation • Customer's current Residential Address • Customer's Signature	• The Legal Name of the Customer • Customer's Date of Birth • Customer's current Residential Address • Customer's ID Type and ID Number	• The Legal Name of the Customer • Customer's Social Security Number or Taxpayer Identification Number, if any • Customer's ID Type and ID Number • Customer's current Occupation • Customer's current Residential Address • Customer's Signature

Customer Due Diligence (CDD)

FinCen's Final Rule on Beneficial Ownership and Customer Due Diligence

The CCD Final Rule stipulates that **covered financial institutions** must implement due diligence procedures that identify and verify a legal entity customer's beneficial owner(s) at the time a new account is opened.

Covered financial institutions include:

- Banking institutions
- Securities-broker dealers
- Futures commission merchants
- Introducing brokers in commodities and mutual funds

A legal entity customer is defined as any corporation, limited liability company, general partnership, or any other entity that is required to file a public document with a Secretary of State or similar office.

The following legal entity customers are excluded from the CDD Final Rule:

- Banking organizations
- Entities that have common stock listed in the New York, American, or NASDAQ stock exchanges
- SEC-registered investment companies and advisers
- CFTC-registered entities
- State-regulated insurance companies
- Legal entities with private banking accounts subject to FinCEN rules

Customer Due Diligence (CDD)

FinCen's Final Rule on Beneficial Ownership and Customer Due Diligence, continued

Beneficial Owner

Under the CDD Final Rule, there are two types of beneficial owners:

- **Ownership prong** - any natural person who owns, directly or indirectly, 25% or more of the equity interests of the legal entity customer
- **Control prong** - any individual with significant responsibilities that include controlling, managing, or directing the legal entity customer (typically the CEO, Vice President, CFO, Treasurer, etc.)

Ouro's Responsibilities Under the CDD Final Rule

Ouro's Compliance Department has implemented procedures to identify and verify the identity of beneficial owners of each legal entity who is opening a new account or maintaining a business relationship with Ouro.

During the course of your relationship with Ouro, your business may be asked for beneficial owner information in order for Ouro to conduct ongoing customer due diligence.

Office of Foreign Assets Control (OFAC)

The Office of Foreign Assets Control (OFAC):

- Enforces economic and trade sanctions against individuals, entities, and foreign governments with interests hostile to the United States
- Publishes a list that identifies those parties with whom transactions are prohibited

The Department of the Treasury updates the OFAC list as necessary, and it includes those suspected of:

- Terrorist financing
- Money laundering
- Narcotics trafficking
- Other crimes
- Governments or organizations with interests hostile to the US

OFAC rules require institutions and their employees to:

- Identify any property or transaction subject to economic sanctions
- Block or reject the transaction
- Freeze an account
- Advise OFAC of the blocked asset or rejected transaction
- Take actions as directed by OFAC
- Release the blocked transaction or property only with OFAC’s authorization

OFAC Noncompliance

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

- Charter forfeiture or loss of insured status
- Monetary losses resulting from asset forfeiture actions and fines
- Substantial legal fees
- Reputational damage and negative publicity

Financial Crimes & Money Laundering

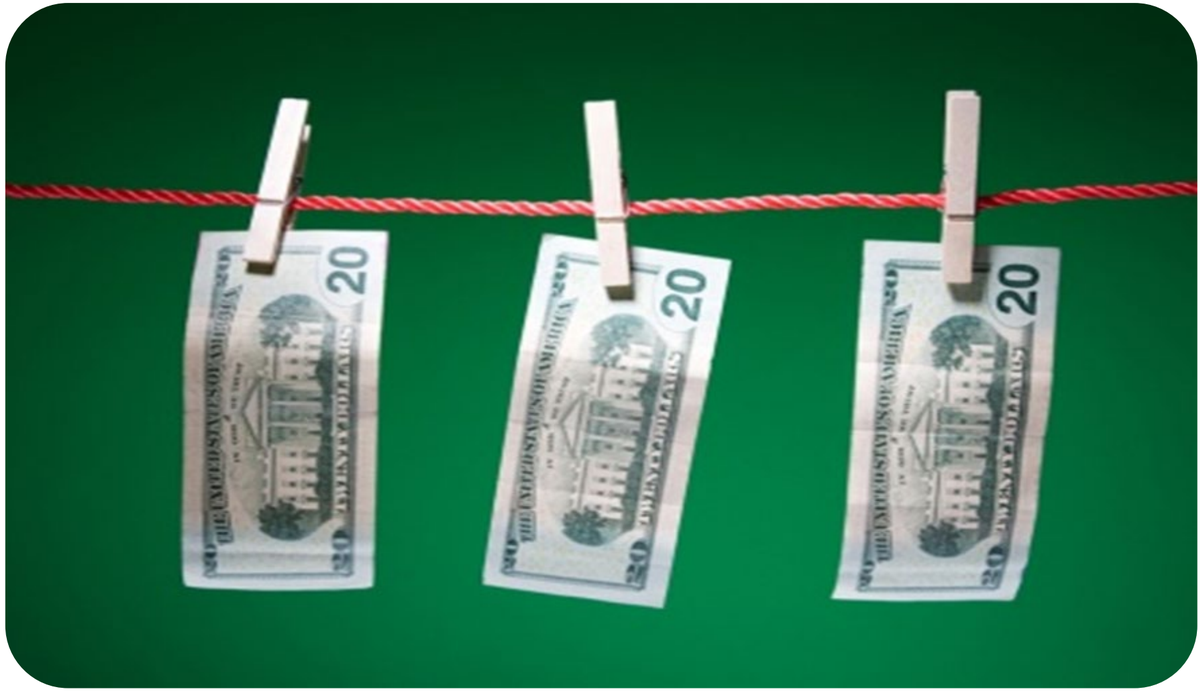
The BSA/AML rules are intended to protect the U.S. financial system and the financial institutions that make up that system from the abuses of financial crimes, such as money laundering, terrorist financing, and other illicit transactions.

Both money laundering and terrorist financing involve criminals exploiting loopholes and weaknesses in the legitimate financial system to launder criminal proceeds, finance terrorism, or conduct other illegal activities, and ultimately hide the actual purpose of their activity.

Money Laundering

Money laundering is the criminal practice of filtering money obtained from illegal activities through a series of transactions so the funds are ‘cleaned’ to appear as though they came from legitimate activities. It involves three independent steps that may occur simultaneously:

- Placement
- Layering
- Integration



Money Laundering Cycle

The 3 Stages

Stage 1: Placement

The money launderer introduces the illegal proceeds into the financial system.

Example: The funds are placed into circulation through financial institutions, casinos, and shops.

Stage 2: Layering

The money launderer converts the proceeds of crime into another form and creates layers of financial transactions to disguise the audit trail, source, and ownership of the funds.

Example: Wire transfers are sent from one account to another.

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 crime.

Example: Funds are invested in real estate, financial ventures, or luxury assets.

Terrorist Financing

Financial Crimes

Terrorist financing provides funds for terrorist activity.

It may involve funds raised from legitimate sources, such as:

- Charitable donations
- Foreign government sponsors
- Business ownership
- Personal employment

Or, it may involve funds raised from criminal sources, such as:

- Extortion and/or kidnapping
- Narcotics
- Trafficking and/or smuggling
- Fraud
- Robbery and/or theft
- Use of conflict diamonds
- Improper use of charitable or relief funds

Detecting Suspicious Activity

Examples of Suspicious Customer Behavior

You must remain on the lookout for potential suspicious behaviors or ‘red flags’ and follow your store’s procedures on how to handle.

Potential Red Flags/Suspicious Customer Behavior

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

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

- All loads to Ouro cards must be performed in person, in exchange for cash/debit ONLY.
- Do not load any Ouro card over the phone, without the funds present.
- Ouro 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.

Suspicious Activity Reporting (SAR)

Definitions & Legal Requirements

Suspicious Activity Report (SAR)

Suspicious activity reports must be electronically filed with the Financial Crimes Enforcement Network (FinCEN) following a suspected incident of money laundering or fraud.

- Required under the Bank Secrecy Act (BSA) of 1970
- Must be kept confidential; do not disclose to anyone that a SAR has been filed

SAR Goals

- Report known or suspected violations of law or suspicious activity observed subject to the regulations of the Bank Secrecy Act
- Help the federal government identify individuals, groups, and organizations involved in fraud, terrorist financing, money laundering, and other financial crimes

MSB Filing Requirements

If your institution is a money service business, then you are responsible for filing your own SARs.

- Refer suspicious activity to Ouro without indicating whether your institution filed a SAR

SAR Filing Deadlines

- Must be reported and filed within 30 days of the initial detection of the suspected violation of law or suspicious activity
- 30-day extension may be granted, if the identity of the person conducting the suspicious activity is unknown

SAR Recordkeeping

Must keep a copy of the SAR and original or business record of supporting documentation used to file the SAR for 5 years

Report Suspicious Activity & Suspected Fraud

Duty to Report

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

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

Report the Activity to the Ouro Compliance Department

- Complete the Unusual/Suspicious Activity Referral form located here: https://www.netspend.com/compliance-guidelines OR
- Contact the Ouro 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 Ouro, or to FinCEN via a SAR report.

Ouro Actions for Suspicious Activity & Suspected Fraud

Duty to Investigate

Once the unusual or suspicious activity is reported to Ouro, we will:

- Review the cardholder's account to determine whether the activity is truly suspicious and requires additional reporting
- Provide your business with feedback on the results of the investigation, as applicable

Remember: SAR filings are confidential. Ouro will not tell you whether a SAR has been filed.

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 on 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.

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.

Potential Red Flags for Elder Abuse

Examples of Suspicious Customer Behavior Indicative of Potential Elder Abuse

Erratic or Unusual Purchases/Transactions or Changes in Account Patterns

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

Interactions with Customers or Caregivers

- 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
- Elder shows an usual 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
- Financial institution is unable to speak directly with the elder, despite repeated attempts to contact him or her
- New caretaker, relative, or friend suddenly begins conducting financial transactions on behalf of the elder without proper documentation
- Elder moves away from existing relationships and toward new associations with other friends or strangers
- Elder's financial management changes suddenly, such as through a change of power of attorney or a different family member or individual
- Elder lacks knowledge about his or her financial status or shows a sudden reluctance to discuss financial matters

Report Elder Abuse

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

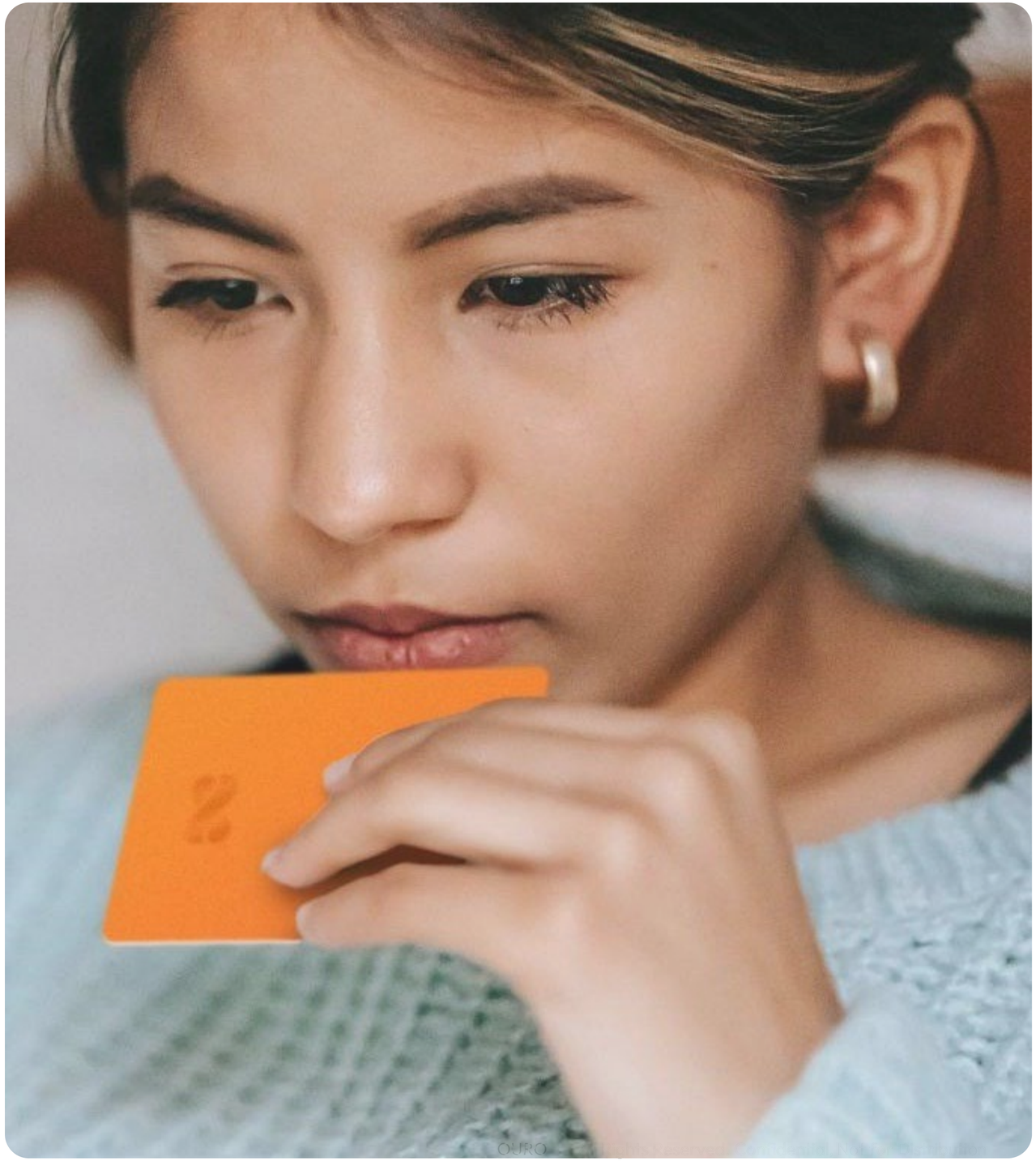
- Local law enforcement
- Local Adult Protective Services (APS) www.eldercare.gov
- FinCEN, via your internal SAR process, as applicable

Note: Your state may have additional reporting requirements.

Report the Activity to the Ouro Compliance Department

- Complete the Unusual/Suspicious Activity Referral form located here: https://www.netspend.com/compliance-guidelines OR
- Contact the Ouro 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 Ouro, or to FinCEN via a SAR report.



Currency Transaction Report (CTR)

Currency Transaction Report (CTR)

A currency transaction report (CTR) is a form required to be completed by financial institutions under the Bank Secrecy ACT (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.

- **Currency** is coin and paper money of the United State, or any other country, which is circulated and customarily accepted as money.
- **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.

CTR Filing Deadlines

- Must be filed electronically with FinCEN within 15 calendar days from the date of the transaction

CTR Recordkeeping

- Must keep a copy of the CTR for 5 years from the date filed

Note: Money Service Businesses (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.

Currency Transaction Report (CTR) Noncompliance

Failure to complete and file a CTR properly, or failure to file a CTR in a timely manner is:

- A violation of the Bank Secrecy Act (BSA)
- A violation of the US Treasury Department regulations
- Subject to severe civil and criminal penalties, including jail time

Additional Penalties May Include:

- Charter forfeiture or loss of insured status
- Monetary losses resulting from asset forfeiture actions and fines
- Substantial legal fees
- Reputational damage and negative publicity

State and Federal Examinations

Examiner Visits

As an agent of Ouro, you are subject to state and federal examinations to verify if your business is compliant with BSA/AML requirements, including implementing Ouro's AML Program requirements.

Periodically, store locations may be visited by a state or federal examiner. It is important to be courteous and to fully cooperate with the examiners. Ouro recommends the following during an examiner visit:

- Be courteous
- Know who your designated compliance officer or compliance contact is
- Direct any questions to your designated compliance officer or compliance contact
- Have immediate access to your AML Program and Ouro's Risk & Compliance Guidelines – this is usually the first item requested at all visits
    - https://www.netspend.com/compliance-guidelines
- Be able to provide current BSA/AML training records
- Be able to facilitate or respond to requests for your AML independent review
- Know where your state posting requirements are located to direct the examiners to view, when applicable

If you are unable to provide the requested information, immediately direct the examiner to your manager and/or designated compliance officer or compliance contact.

Key Points to Remember

- Your agent and distributor responsibilities
- Basic understanding of the Bank Secrecy Act (BSA)
- Importance of the Customer Identification Program (CIP) and OFAC
- Basic understanding of financial crimes, money laundering, and terrorist financing
- Examples of suspicious customer behavior
- Your duty to monitor and report suspicious customer behavior
- Follow your SAR and CTR filing procedures, if you are an MSB
- All loads to Ouro cards must be performed in person, in exchange for cash

Ouro will **NEVER** contact you to ask you to:

- Load funds onto Ouro cards over the phone, without the funds present
- Load funds to ‘test’ a card
- Download software or updates to your computer
- Provide or ask for username and/or passwords to your systems

Important Contact Information

Ouro Support

For use by your staff ONLY

Ouro Partner Services:
1.866.397.5643
Hours of Operation:
8AM to 10PM CST, Monday – Friday
8AM to 6PM CST, Saturday
9AM to 5:30PM CST, Sunday
Email: partnersupport@netspend.com

Ouro Compliance Department:
1.866.914.7224 (p); 512.539.5839 (f);
Email: compliance@netspend.com

For customer use:

Ouro Customer Service:
1.86.Ouro (1.866.387.7363)
I.V.R hours: 24/7
Live Agent Hours of Operation:
8AM to 10PM CST, Monday – Friday
8AM to 8PM CST, Saturday & Sunday
Email: customerservice@netspend.com

ouro reinvent possibilities

Thank You.

reinvent possibilities