TransCash Anti-Money Laundering (AML)

Compliance Program Guide

Table of Contents

1. Objectives of Guide
2. Introduction
3. Summary of AML Compliance Program
4. KYC Policy
5. Structuring Policy
6. Red Flag Policy
7. Recordkeeping Policy
8. Suspicious Activity (SAR) Rules
9. Civil and Criminal Penalties
10. FinCEN Form 109 *(to be added in January 2012)*
11. TransCash Red Flag Form
12. TransCash Non-Responsive Form
13. Independent Review Form
14. AML Training Completion Form
15. AML Update Session Form
16. **OBJECTIVES**

* Detect and prevent money laundering and terrorist financing;
* Comply with the BSA requirements
* Comply with the USA PATRIOT ACT;
* Identify and report suspicious activity;
* Comply with the requirements of the Office of Foreign Assets Control (OFAC) and other Anti-Money Laundering (AML) regulations.

Please note that your knowledge of the information described in this Guide may

* + help prevent TransCash from being victimized by money launderers and
  + help you, as an employee of TransCash, comply with the law.

In addition, please keep in mind that your efforts and compliance with the requirements in this guide may help law enforcement agents in their efforts to track down and capture terrorists who illegally launder money.

1. **INTRODUCTION**

**What is a Money Services Business (MSB)?**

According to the Financial Crimes Enforcement Network (**FinCEN**), TransCash is a Money Services Business (**MSB**). FinCEN is a bureau of the U.S. Department of the Treasury that administers and issues regulations pursuant to the Bank Secrecy Act (**BSA).** A business is considered a Money Services Business (MSB) if the business offers one or more of the following services:

* money orders
* traveler’s checks
* check cashing
* currency exchange
* **prepaid access**
* money transfer services

At TransCash, we fall under the category of **Prepaid Access.** Therefore, we need be compliant with BSA regulations. The main component of MSB regulations is the TransCash Anti-Money Laundering compliance program.

**What is Money Laundering?**

Money is “laundered” to conceal illegal activity, including the crimes that generate the money itself, such as drug trafficking. Money laundering conceals the source of illegal proceeds so that the money can be used without detection of its criminal source.  
  
Money Services Businesses (MSB) have been both witting and unwitting participants in laundering activities. MSBs have been major targets in laundering operations because they provide a variety of services such as money orders, traveler’s checks, money transfers, check cashing, currency exchange, and stored value services which can be used to conceal the source of illicit proceeds.  
  
To protect ourselves, and to support national and international efforts against financial crime, it is important that TransCash and its employees know how money laundering schemes can operate. This TransCash Anti Money Laundering Compliance Program (TransCash AML Compliance Program) contains the basic policies and procedures needed for TransCash to be compliant with federal regulations. The federal government, using the Bank Secrecy Act and the Money Laundering Control Act, has written strict laws and regulations to help prevent money laundering activities.

**What is an Anti Money Laundering (AML) Compliance Program?**

TransCash is required by law to have an effective Anti-Money Laundering (AML) compliance program in order to stay compliant with FinCEN regulations. An effective AML compliance program is one designed to prevent TransCash from being used to facilitate money laundering.

In this handbook, you will find the required information to run the TransCash AML Compliance Program which includes:

* TransCash’s policies, procedures and internal controls reasonably designed to assure compliance with the Bank Secrecy Act (BSA),
* Information of who your compliance officer ,
* The proper material to keep you informed on your responsibilities under the TransCash AML Compliance program as an employee.
* The necessary form to submit to the Customer Service Manager and Compliance Officer.

Please note that TransCash keeps informed of FinCen Regulations’ updates and therefore, you will be asked, when needed, to read and confirm understanding of new and updated regulations.

TransCash has a comprehensive compliance program within its organization to ensure compliance with government rules and regulations. We do not want TransCash Prepaid Debit Card services to be used in illegal money laundering activities. It is our policy that we follow both the letter and the spirit of the law and the regulations.

TransCash does not allow money transfers intended for gaming, gambling or illegal activity. We will stop all identified transfers associated with any such activity.

1. **SUMMARY OF AML COMPLIANCE PROGRAM**

TransCash and all its employees strictly follow the compliance program to prevent criminals from laundering money that comes from illegal activity.

Keeping track of transactions and customers that are transferring money from Cards to Cards and in other countries is important because we want to make sure that no customer goes undetected through our system, these policies are according and compliant with FinCEN and Patriot Act.

In brief TransCash employees are expected to comply with the following policies:

**NOTE:** This page is a brief summary of the policies and does not replace the information included in this program. Please make sure you **thoroughly read** the program and understand what is expected from you as a TransCash employee.

* **Know Your Customer (KYC) Due Diligence**

It is important for TransCash to know who we sell our cards to. Customers will be buying our cards online and at retailers therefore this step of the activation process is very important. This means that we do not have face to face customer relationship and gathering the proper information over the phone and proper copies of valid IDs is crucial to our KYC policies and due diligence. Establishing this initial relationship can help us determine the quality of customers we have and reassures the customers of the quality of service we provide. Lastly, KYC helps us report any suspicious customer that may be involved in illegal transactions and is trying to use our cards as a cover up, with this we work close with FinCEN.

* **Structuring**

As a TransCash employee you will have access to customers’ accounts and their card activity. It is important to learn what the “usual” transactions customers do are and what are suspicious transactions. The law says any transaction of over $10,000 has to be reported to the government. For MSBs any transaction over $2,000 must be reported to the government. Therefore, here at TransCash we use our card limitations of $950 per load and try to detect if customers are trying to purposely stay away from the limits by breaking up transfers or loads to cards. The section on structuring will go more into details with examples.

* **Red Flags**

TransCash has two levels of reporting; the first is Red Flag Reports the second are SARs which will be explained in the next bullet point. As an employee who has everyday contact with customers, it is important to know your Red Flags and know when to report Red Flags to Customer Service Manager (CSM) and Compliance Officer.

* **Suspicious Activity Report (SAR)**

A SAR is the second and more serious level of reporting here at TransCash. This report is filed by the Compliance Officer after a Customer Service Representative (CSR) submits a Red Flag Report. This means the Red Flag report was reviewed by the Customer Service Manager and needs further investigation and reporting to FinCEN. Compliance Officer will take care of procedures from here.

* **Reports**

After reading carefully through all the risks and red flags here at TransCash you will be able to detect when to submit a Red Flag Report. The Red Flag Report is especially designed for the Customer Service Manager and Compliance Officer to further investigate questionable customer transactions or things that you do not understand. You will have access to customer accounts and will be logging in to their transactions on a daily basis therefore sometimes you may see things that cannot be easily spotted by Management. All of your inquiries will be taken into consideration and your cooperation is greatly appreciated in advance.

1. **KYC POLICY**

The “Know Your Customer” due diligence is a key element of the AML Compliance program. As a TransCash employee, it is your duty to understand and implement all of the KYC procedures in order to properly screen new customers and confirm they are not involved in terrorist or illegal activity according to the Patriot Act and FinCEN.

The CSR needs to do the following once a customer purchases the dual pack of prepaid debit cards:

* collect Cardholder information
* fill out CardWIZ
* verify the customers information which includes:
  + - Cardholder Name
    - Cardholder physical address, phone[[1]](#footnote-1), email
    - Cardholder date of birth
    - Cardholder Social Security Number (SSN)
    - In the absence of or in addition to an SSN, alternative forms of identification may be permitted with the permission of the Bank.
    - Identity documents
    - U.S. visa for work or study
    - INS-approved green card or other work permit;
    - Mexican Matricular
    - Other U.S.-issued tax identification number (TIN)
    - Government issued ID/Passport (U.S. or non-U.S.)

This Cardholder information will be entered into the CardWIZ data base as ***Submit for Approval*** and will be verified through a recognized identification verification source, such as Veratad. OFAC verification must also be performed monthly, at minimum.

**A copy of the proper ID needs to be requested and turned in to your Customer Service Manager. Remind customers that cards will not be activated until TransCash receives a copy of the ID and all their information has been verified.**

Cardholders may have the option of providing additional information in the event that a match cannot be made through any of the above sources.

**TransCash Card are issued as an “Instant Issue Card”**

The Instant Issue Card has a generic “name” embossed on the card – “Preferred Customer” for TransCash. This appears as an anonymous card but, prior to issue, TransCash must verify the “Know Your Customer” (KYC) provision. This generally speeds the sale, value loading and activation process, expediting the point-of-sale experience for customers and retailers. TransCash Cards are bulk ordered and then offered to consumers in retail locations. Cards are provided to the consumer upon purchase and are activated once the KYC procedures are completed over the phone through TransCash customer service. The cardholder is able to use the Card anywhere that Visa Prepaid Card is accepted worldwide.

**Tracking new cards activated after KYC:**

After KYC has been verified and approved, cards are activated by customer service here at TransCash headquarters.

At the end of each day, CSR Manager will:

* Create a list of GPR cards that were verified and activated with initial load amounts

This report needs to be reviewed by the Compliance Officer who will:

* Update the TransCash inventory list with cards sold.
* File the IDs of the new customers for that day electronically and physically at headquarters.

1. **STRUCTURING POLICY**

TransCash does not allow structuring transactions of any type or any amount. We are constantly working together to detect if any TransCash customers attempt to structure transactions. It is illegal for a customer to structure transactions and as a TransCash employee is it is your duty to report and submit a Red Flag form[[2]](#footnote-2) for CSR Manager and Compliance Officer to review.

The US government has established reporting requirements for anyone who transfers more than $10,000. FinCEN has established similar reporting requirements for MSBs that transfer more than $1,000; these regulations are used to monitor large amounts and prevent illegal transactions. Criminals try to bypass these reporting regulations and break up payments. At TransCash, as an MSB, our internal limits are as follows:

* TransCash only allows a maximum of **$950** to load per day
* 50 Transactions per cycle
* 30 days in a cycle
* Maximum ATM withdrawal per transaction $500
* Minimum ATM withdrawal per transaction $20
* 5 transactions in ATM per day

**What is structuring?**

Many money launderers are familiar with the dollar thresholds that require recordkeeping and reporting. Therefore, in order to remain anonymous and avoid the detection of TransCash or law enforcement officials, criminals will “structure” their transactions so reporting will not be triggered.

Structuring is the act of **breaking up** potentially large transactions into several smaller ones to avoid reporting or recordkeeping requirements by TransCash or FinCEN.

**EXAMPLE 1:**

TransCash only allows a maximum of **$950** to load per day:

Lets assume the customer knows about the maximum load amount and knows that reports are administered if customers attempt to do transactions larger than $950, therefore they want to stay “off the radar of TransCash.”

* Customer loads $475[[3]](#footnote-3) at one Visa ReadyLink location
* Customer loads $475 at another Visa ReadyLink location that same day
* Withdraws transfers and withdraws the $950 at an ATM with the Secondary (Red) card.
* Customer does this consecutively on more than **2 days**

This sort of activity should raise a red flag and should be reported to the Manager with a Red Flag form completely filled out.

**EXAMPLE 2:**

TransCash only allows a maximum of **$950** to load per day:

* Customer loads anywhere from $300-$950 Bank to Card and withdraws same day
* Customer loads $300-$6950 Bank to Card and withdraws again on the same day.

This sort of activity should raise a Red Flag and a report should be turned in to the Manager.

**Patterns that show consistent amounts and withdraws need to be reported to the Manager because customer may be trying to structure transactions in a way where they want remain unseen and not tracked.**

**VERY IMPORTANT: IT IS AGAINST THE LAW TO NOTIFY CUSTOMER THAT THEY ARE BEING RED FLAGGED.**

**NOTE:**

It is also illegal for employees to assist anyone in structuring transactions by avoiding recordkeeping or reporting requirements. For example, you may not tell or even imply to a client that they can avoid providing information by conducting a smaller transaction.

**Also be aware of:**

Some criminals may attempt to trick the employee into allowing them to structure transactions by splitting up their activity with several accomplices or by trying to “con” you with a hard luck story. You need to be on the lookout for structuring so that you prevent it from occurring when transferring funds from Card to Card.

1. **RED FLAG POLICY AND IDENTITY THEFT PREVENTION PROGRAM**

As per the “Red Flags” Rule, in effect since January 1, 2008, the TRANSCASH Identity Theft Prevention Program is designed to prevent, detect, and mitigate identity theft in connection with the opening of new accounts and the operation of existing ones.

The TRANSCASH Identity Theft Prevention Program is A FOUR STEP PROCESS which includes:

* Identify relevant red flags.
* Detect the warning signs – or “red flags” – of identity theft in the business day-to-day operations.
* Take steps to prevent the crime by Setting up procedures to detect those red flags in the day-to-day operations to prevent and mitigate identity theft.
* Update the Program.

**IDENTIFY RELEVANT RED FLAGS AND STEPS TO TAKE IN CASE OF RED FLAG WARNINGS**

Red flags are alerts that TransCash employees need to be aware of and implement in their every day calls when talking to customers or when treating online orders. Identifying proper red flags can prevent fraud and money laundering crimes.

1. **Red Flags when dealing with a NEW customer:**



1. Customer changes name when asked to send a copy of proper ID.
2. You suspect or know the ID is fake.
3. A customer threatens or bribes an employee in order to avoid providing information.
4. You dealt in one day with two or more customers using similar IDs.
5. Be suspicious of customers who do not provide phone numbers and full addresses.
6. Beware of diplomatic passports from obscure countries – particularly ones in Africa where such passports can easily be obtained by paying for them. The passport may be genuine (i.e. genuinely issued after payment), this does not mean that the holder is genuine or the name shown on the passport is the real one. Obviously another aid in this type of scenario is to try and evaluate whether the **other** details given, together with the appearance/attitude of the person, match whatever diplomatic post he/she is claiming to hold
7. Customer alters activation information or money sharing amount upon learning he/she must have a proper ID.
8. Customer asks if they can remain anonymous.
9. Be suspicious if a group of accounts are opened by foreign nationals who call to activate TransCash cards on the same day. Be aware if all purchases are coming from the same retailer.
10. Suspicions should be aroused if multiple cards are activated by an individual using the same address, or different individuals using the same address
11. Suspicions should result if numerous customers are trying to activate their TransCash Card using variations of the same name
12. Suspicions should be aroused if customer asks for the TransCash card to be shipped to an address which does not match the one on his/her ID
13. Suspicions should be aroused if customer provide Suspicious Personal Identifying Information which show inconsistencies such as:
    1. date of birth does not match the picture, or a date of birth that doesn’t correlate to the number range on the Social Security Administration’s issuance tables
    2. an address, phone number, or other personal information that’s been used on an account you know to be fraudulent
    3. a bogus address, an address for a mail drop or prison, a phone number that’s invalid, or one that’s associated with a pager or answering service
    4. a Social Security number that’s been used by someone else opening an account
    5. an address or telephone number that’s been used by many other people opening accounts
    6. a person who omits required information on an application and doesn’t respond to notices that the application is incomplete
    7. a person who can’t provide authenticating information beyond what’s generally available from a wallet or credit report – for example, a person who can’t answer a challenge question

When coming across any of the **Red Flags A-M** immediately follow the following procedures:

**Step 1: VERY IMPORTANT: IT IS AGAINST THE LAW TO NOTIFY CUSTOMER THEY ARE BEING RED FLAGGED.**

**Step 2:** Ask customer for **2** contact numbers where they can be reached.

**Step 3:** Fill out information on CardWiz and press “**Submit for Approval.”**

**Step 4:** Advice customer that management will review information for verification purposes and they will be contacted shortly.

**Step 5:** Immediately fill out the Red Flag form and submit to Manager**.**

Once Red Flag form is submitted, Manager will follow appropriate procedures:

* Review information and the employees comment.
* Verify names and addresses in TransCash’s Red flag database.[[4]](#footnote-4)
* Contact customer and verify information and attempt to get valid ID.

**Resolution Procedures:**

* Check what city, state and store card was purchased
* Check what address the ID shows
* Check what address customer was trying to use for the CSA profile
* Check the address IF CC was used
* Check contact numbers; call and verify with cardholder
* If they sent a copy of the ID, check the IP address
* Check information against previously declined order
* If problem was solved by the Manager and the misunderstandings were cleared, Manager can proceed with the activation and approve order.
* Manager will sign and date Red Flag form and submit to Compliance Officer for TransCash Record keeping policies.

**IN CASE OF NO APPROVAL:**

* Manager will notify customer that their order cannot be processed due to failure to successfully pass the verification and security measures here at TransCash.
* Manager should verify the Credit Card being used for loading and make sure it is not stolen.
* Customer will be notified that they have not been approved. Therefore, their card will only be temporary and not reloadable. They will be able to use the card until all funds have been withdrawn. **NOTE:** this is a pending hybrid program, IT is working on adding this feature to our card program.
* Manager will sign; date and state resolution on the Red Flag form and give to Compliance Officer for proper filing.

1. **Red Flags when dealing with existing customers:**



1. You notice customer never uses primary card (Black); they always call to share **ALL** funds after a load onto secondary card (Red). ( they only transfer and withdraw money)
2. You notice customer never makes purchases; they **only** withdraw money after loads.
3. Customer calls for ex. for a balance inquiry and you notice in the activity they have more than **4 ATM or Purchase decline.**
4. If you are in the customer’s account information and you notice they changed their address or contact information.
5. If you notice the customer withdraws cash from ATMs in a “structured[[5]](#footnote-5)” way using TransCash limits. For example: they withdraw always the maximum allowed, $500 from ATM day 1, $500 from ATM day 2 etc.
6. You notice they never leave enough money in the Primary card (Black) to cover the monthly fee of $9.99 for **2 consecutive months.**
7. A customer asks an employee how to avoid a reporting requirement.
8. Soon after you’re notified of a change of address, you’re asked for new or additional credit cards, cell phones, etc., or to add users to the account
9. an account that’s been inactive for a long time is suddenly used again
10. Sometimes a red flag that an account has been opened or used fraudulently can come from a customer, a victim of identity theft, a law enforcement authority, or someone else.

When coming across any of the **Red Flags N-W** immediately follow the following procedures:

**Step 1:** **VERY IMPORTANT: IT IS AGAINST THE LAW TO NOTIFY CUSTOMER THAT THEY ARE BEING RED FLAGGED.**

**Step 2:** Verify the customer’s contact number.

**Step 3:** Immediately fill out the Red Flag form and submit to Manager**.**

Once Red Flag form is submitted, Manager will follow appropriate procedures:

* Review information and the employees comment.
* Verify names and addresses in TransCash’s Red flag database.
* Contact customer and verify information to find a resolution.

**Resolution Procedures:**

* Manager was able to:

1. Indentify Problem and made a note of it on the Red Flag sheet
2. Then found a resolution with customer

* Once resolved, Manager will sign and date Red Flag form and submit to Compliance Officer for proper filing.

If, Manager needs further assistance with transaction verifications then issue will be forward to Compliance Office and IT department for further investigation. Compliance Officer will take appropriate measures;

* Verify information and dismiss if solved.
* Confirm the problem as a legitimate Red Flag and cancel transaction/customer.
* Determine if customer activity needs to be submitted as an official SAR.[[6]](#footnote-6)

**3. Falcon FIS Red Flag**



Transactions also get monitored by the FIS (our processor) Falcon Fraud Detection Service software. The software is designed to monitor illegal transactions when it detects a fraudulent transaction based on the Flacon scores FIS has full authority to block such a transaction or authorization request.

This Falcon Red Flag is an internal Red Flag, Compliance Officer and management will keep track of any transactions of customers that were flagged by the FIS Falcon program.

4**. Veratad Technologies Red Flag**



Veratad Technologies, LLC is a provider of both online/real-time and batch Identity Verification and Knowledge Based Authentication Solutions for those who conduct business on the Internet or any business that needs to verify an individual's age or identity.  Their verification Solutions are designed to verify an individual’s identity and/or age while protecting sensitive personal data and promoting a high level of consumer privacy.

TransCash subscribe to the following solutions:

**1. IDMatch - Identity Verification**

***IDMatch*** *is an advanced Identity Verification Search Technology running on Veratad's IDresponse Secure Data Platform through Real-time API Web Service, Virtual Terminal or Custom Batches.*

*The system scans billions of records to locate and confirm identity based on information submitted by consumers and/or businesses.*

*This service offers a powerful, real-time Identity Data Validation in just seconds for US based Identity Verification and International Identity Verification.*

*All this while we protect sensitive data and consumer privacy with our patent pending privacy tools that will allow you to offer your customers an option to fully protect their Social Security or other alphanumeric information such as credit card and phone numbers. For example, when verifying identity you can use our privacy tools to protect Social Security Number information by asking only for a random sum of just two included numbers rather than the customary full or last four digits. IDMatch +PLUS is the perfect solution for your* [*Red Flags Rule Compliance*](http://veratad.com/Red_Flag_Rules__Solutions.html) *and* [*FFIEC Authentication*](http://veratad.com/compliance_FFIEC_guidance_out_of_wallet_Challenge_questions.html) *Guidelines.   
  
In addition, our user defined security settings allow you to define data access levels for employees.*

**2. IDMatch+PLUS** **Knowledge Based  Identity Authentication**

**IDMatch+Plus** is Veratad's IDMatch Solution with an added layer of consumer challenge that includes our User Defined Knowledge Based Historical Questions Sets.

These non-intrusive questions are easily added to IDMatch when you need an enhanced Authentication Solution.

The system is designed so you decide the number and nature of the questions, then build your own business rules for adjudication.

The system scans billions of records to locate and confirm identity information that is submitted by consumers and/or businesses.

This service offers a powerful, real-time Identity Authentication in just seconds.

**SUMMARY OF BENEFITS**

**Veratad's ID Verification and Quiz Solutions for IDMatch and IDMatch+PLUS on the IDresponse Privacy Processing Platform offers the following benefits:**

1. Shows the company is vigilant about Due Diligence in preventing Fraud and ID Theft
2. Does not require sensitive personal information for verification
3. Automates Validation in Real-time Through Online or Offline, Mobile Devices and Kiosks
4. No storage of sensitive personal information
5. Comply with rules and regulations of the USA Patriot Act, OFAC, and Bank Secrecy Act
6. Excellent solution for FACT Act Compliance Identity Verification component for any entity looking to reduce risk and protect their business and clients from fraud.
7. IDMatch+PLUS Dynamic Out of Wallet Challenge Questions is an excellent replacement for Static Challenge for FFIEC Authentication Compliance
8. Reduces Credit Card Charge Backs to Merchants Social Security Number Verification
9. Flexible API Integration or Access via our Web based Virtual Terminal
10. Access to All Transaction Data via our Proprietary Web Interface
11. Compliant with SSN Act,  Customer Privacy Act, DPPA, FCRA, Graham Leach-Bliley Act ,COPA and COPPA

**UPDATE THE PROGRAM**

TransCash is aware that new red flags emerge as technology changes or identity thieves change their tactics. Therefore, our Program is periodically updated to ensure that it keeps current with identity theft risks. We take into account the following:

* Factor in our own experience with identity theft;
* Changes in how identity thieves operate;
* New methods to detect, prevent, and mitigate identity theft;

An annual review of the program is schedule on March 12 of each year.

1. **RECORDKEEPING POLICY**

Recordkeeping is important because these files need to be readily accessible in case TransCash is ever examined and/or audited by regulators. Your cooperation is very important to help continue the success of the TransCash AML compliance Program.

It is TransCash policy to record and submit the following to the Manager:

1. **A $100 initial load**

When a customer first purchases a TransCash Prepaid Debit card they have the option of loading the card with:

* $20, $50 or $100 in addition to the $9.99 fee they must pay

The most common initial load at TransCash is $20, usually a customer wants to test the new product. If a customer calls to activate cards and you see their initial load was $100 please fill out the Red Flag form and submit to Manager for TransCash recordkeeping purposes.

Manager will:

* Call with a TransCash Welcome call[[7]](#footnote-7) and verify amount and purchase.
* Resolve suspicion and submit Red Flag form to Compliance Officer for TransCash filing

**OR**

* Confirm as a legitimate Red Flag and inform Compliance Officer in order to take appropriate action; Cancel/Suspend Customer and file document.

1. **Transactions of $950**

A customer will never have an **initial load** of $950 because the maximum is $100. However if at any point a customer calls to make a **transfer** of $950 to their companion card you need to fill out a Red Flag form and submit to Manager for TransCash recordkeeping purposes.

**NOTE:** It is **not illegal** to make transactions, transfers, withdrawals, or loads of $950. The $950 is a TransCash internal card limit. It is also **not illegal** to make transactions, transfers, withdrawals or loads of $2,000 MSBs just need to record and report transactions of $2,000 or $10,000 for precautionary measures.

CSR Manager will:

* Review the customers’ usual behavior through CSA and determine if this is a common transfer of funds.
* Determine that there are not illegal transactions.
* Dismiss issue and submit to Compliance Officer for filing.

**OR**

* Advice Compliance Officer that further investigation must be done. Compliance Officer will proceed with appropriate actions: Dismiss issue or Cancel customer and file documents.

**NOTE:** These reports will be stored for TransCash internal Recordkeeping for up to 5 years. TransCash requests to attach the CSA TransCash Cardholder customer information form with the Red Flag form reports to have complete information.

1. **Copy of IDs**

Part of the KYC due diligence is to request a copy of a proper ID that clearly shows the customers:

* Name
* Address
* DOB
* State issued
* Expiration Date

It is TransCash policy to maintain a record of new customer IDs for up to 5 years and update every time there is a change.

It is important that you submit the IDs to your CSR Manager at the end of the day.

Manager will:

* Review IDs and check they are legitimate.
* Submit to Compliance Officer for proper filing.

1. **SUSPICIOUS ACTIVITY RULES**

The federal government requires TransCash to file a Suspicious Activity Report (SAR-MSB) for any transaction – or pattern of transactions – that is attempted or conducted with at least $2,000, that Customer Service Representative knows, suspects or has reason to suspect:

**1.** Involve funds derived from illegal activity or is intended to hid funds derived

from illegal activity;

**2.** Is structured to avoid recordkeeping or reporting requirements;

**3.** Has no business or apparent lawful purpose; or

**4**. Facilitates criminal activity.

A SAR-MSB can also be filed on suspicious activity below $2,000, but the regulations do not require it.

**Filing Requirements for SAR-MSBs**

TransCash must file a SAR-MSB within 30 days of detection of the suspicious event. The SAR-MSB must be mailed to the address on the form or E-filed through FinCEN.

**At TransCash, the SAR will be filed by Management and Compliance Officer. Please notify your CSR Manager immediately if for any reasons, you suspect the customer to be involved with illegal transactions.**

Management and Compliance Officer will:

* Review customer transactions
* Determine whether a SAR needs to filed with FinCEN
* File away the initial request or the file the actual SAR if submitted to FinCEN

**Recordkeeping for SAR-MSBs**

TransCash must keep a copy of each SAR-MSB for at least five (5) years.

**Never Tell Your Customer that You Filed a SAR-MSB**

It is illegal to tell a customer that you are filing a SAR-MSB or a Red Flag form. If TransCash believes that customers may be misusing the TransCash Cards our compliance staff will take proper action. TransCash does not allow money transfers intended for gaming, gambling or illegal activity. We will stop all identified transfers associated with any such activity.

1. **CIVIL AND CRIMINAL PENALTIES**

The government can impose harsh civil and criminal penalties against anyone who violates the BSA, USA PATRIOT Act, OFAC or other anti-money laundering laws and regulations. Civil and criminal fines can quickly reach into the hundreds of thousands or even millions of dollars. The criminal penalty for violating a BSA requirement is a fine of up to $500,000, a jail term of up to 10 years, OR BOTH.

Under certain circumstances, businesses can be held criminally liable for the acts of their employees; it is important for your employees to be trained in these matters and for your business to have a system in place to ensure employees’ compliance with the laws and regulations. If you or your employees do not comply, you may be subject to large fines and/or imprisonment.

The government requires strict compliance with these laws and regulations. TransCash will immediately terminate employment of anyone who knowingly fails to comply with the laws and regulations. TransCash does not allow money transfers intended for gaming, gambling or illegal activity. We will stop all identified transfers associated with any such activity.

* If you suspect terrorist financing, you should immediately report the incident to the Manager and Compliance Officer for them to report it to FinCEN hotline at **1-800-556-3974**, which is operated 24 hours a day, seven (7) days a week. TransCash Management will also file a SAR-MSB on any suspected terrorist activity.
* The Financial Action Task Force (**FATF**) and FinCEN have both issued guidance on financial transactions that may be indicative of terrorist financing at [www.fatf-gafi.org](http://www.fatf-gafi.org) and [www.fincen.gov](http://www.fincen.gov).
* **OFAC** is part of the **U.S. Department of the Treasury** and is responsible for enforcing U.S. government sanctions programs against countries, organizations and individuals.

Sanctions programs typically involve blocking assets to further national security. Many of the sanctioned individuals, commonly referred to as “SDNs,” are drug dealers and terrorists. All U.S. entities are prohibited from conducting any financial transactions with SDNs. You can learn more about OFAC by visiting the Treasury Department’s website at [www.ustreas.gov/offices/enforcement/ofac](http://www.ustreas.gov/offices/enforcement/ofac). The site also includes an extensive list of questions and answers to common questions regarding OFAC.

* **The Financial Crimes Enforcement Network (FinCEN)** is a bureau within the U.S. Treasury Department that administers the federal government’s anti-money laundering laws and regulations. Regularly review FinCEN’s website for MSBs ([www.msb.gov](http://www.msb.gov) ) updates.

1. **FINCEN FORM 109**

Form 109 is the official form from FinCEN to report Suspicious Activity. This form can be easily accessed from the FinCEN website; also Compliance Officer always has extra copies.

However, at TransCash if SAR need to be filed they will be done electronically through the FinCEN e-filing system. This form can serve as reference only. **11. TRANSCASH RED FLAG (POTENTIAL SAR)**

**Purpose:** The client on this list has been flagged as suspicious due to (check all that apply):

* The initial load amount
* KYC problems
* You noticed structuring in the customers activity
* You noticed customer is not properly using their TransCash card
* Other\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Compliance Department will:**

1. Double check and verify the information on this customer
2. Review activity on the card
3. Monitor Customer as needed; Daily or Weekly

|  |  |
| --- | --- |
| **Name of Customer** |  |
| **Card Number & Location of Retailer** |  |
| **Date reported** |  |
| **Customer Reps Name** |  |
| **Reason for Flagging**  **(Details)** |  |
| **Approval by CS Manager & Date** | Comments: |

***Please Note: It is illegal to tell any person involved in a transaction that a SAR or “Hot List Flag” has been reported to management. Maintaining the confidentiality is part of your duty.***

**12. TRANSCASH NON-RESPONSIVE CUSTOMERS**

**Purpose:** The client on this list has been flagged because:

1. The client has not activated his/her cards (after 2 months of purchase).

OR

1. The client activated his/her card but has never used it and money is sitting in the account (after 2 months of purchase).

**Customer Service Manager will:**

1. Contact the customer via:
2. E-mail
3. Telephone: Cell & Home
4. Mail if unable to contact otherwise

|  |  |
| --- | --- |
| **Name of Customer** |  |
| **Card Number** |  |
| **Date reported** |  |
| **Customer Reps Name** |  |
| **Reason for Flagging**  **(Details)** |  |
| **Resolution by CS Manager & Date** |  |

**13. AML- INDEPENDENT REVIEW**

This is to certify that on ­­­­\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ the TransCash Independent Review was conducted by \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ at the designated location: 1801 Avenue of the Stars, Suite 1444 Century City, 90067.

By signing this form, I certify that the following aspects of the TransCash AML program were verified:

* The Compliance Officer has updated procedures for rules and regulations regarding the AML program according to FinCEN.
* The Compliance Officer is properly keeping records of new and continuous customers and of filed or resolved potential SAR issues.
* The Compliance Officer has a yearly mandatory training program in place for employees and schedules meetings if necessary to update employees.
* The Compliance Officer has a hard copy of the AML manual available for employees upon request.
* The Compliance Officer has a new file with the continuous policy changes and updates from FinCEN.
* All employees of TransCash have attended and signed the AML Training Completion form.
* All employees dealing directly with customers have a copy of TransCash Red Flags alerts and KYC procedures in a visible place at their desk where it can easily be accessed.
* All employees have a copy of the TransCash AML Program.
* There is an established “check and balance” between the Compliance Officer and the Customer Service Manager.
* Compliance Officer checks and verifies new customers and activity reports on a weekly basis and records check-ups as stated in the TransCash AML program.

Please insert notes and comments if needs be:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

I will act with high ethical standards in compliance with laws and regulations governing financial transactions here at TransCash and the AML yearly Independent Review.



**14. ANTI MONEY-LAUNDERING TRAINING PROGRAM**

This form is to confirm that I have attended the mandatory Anti-Money Laundering training program for TransCash that took place on \_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the TransCash Headquarters, located at 1801 Avenue of the Stars, Suite 1444 Century City 90067.

By signing this form, I declare that I have read and understood the following facts:

* What is Money Laundering
* What are the TransCash Red Flags
* What are the TransCash KYC procedures
* When to file a SAR
* Procedures to follow in order to file a SAR
* How to submit a suspicious activity to TransCash management

I understand that this information is confidential under the BSA Act. I will act with high ethical standards in financial transactions and compliance with laws and regulations governing financial transactions here at TransCash.



**15. ANTI MONEY-LAUNDERING UPDATE SESSION**

This form is to confirm that I have attended the mandatory Anti-Money Laundering **Update Session** for TransCash that took place on \_\_\_\_\_\_\_\_\_\_\_\_\_\_ in the TransCash Headquarters, located at 1801 Avenue of the Stars, Suite 1444 Century City 90067.

By signing this form, I declare that I have read and understood the new **FinCEN updates:**

* I have a copy of the new updates, if needed
* I understand the new procedures, if changes were made

I understand that this information is confidential under the BSA Act. I will act with high ethical standards in financial transactions and compliance with laws and regulations governing financial transactions here at TransCash.



**CONTACTS**

If you have any questions or do not understand any of the policies and procedures please contact your Customer Service Manager or Compliance Officer. They will be able to provide you with further assistance and answers to questions.

**Customer Service Manager**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Compliance Officer**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

1. Please make sure phone numbers are working numbers. Call back and verify. [↑](#footnote-ref-1)
2. Please see Exhibit 1 for Red Flag Form [↑](#footnote-ref-2)
3. Please note these amounts are hypothetical amounts and serve the purpose of an example; be aware the range can be from $1.00-$950.00 your responsibility is if you notice a pattern or a questionable transaction to report it to Management. [↑](#footnote-ref-3)
4. Compliance Officer will have a database with a list of Red Flagged customers to easily look up names. [↑](#footnote-ref-4)
5. Please see Chapter on **Structuring** for more information. [↑](#footnote-ref-5)
6. SAR- Suspicious Activity Report- Filed through FinCEN [↑](#footnote-ref-6)
7. CSR Manager wants all new customers to be greeted with a Welcome Call after activation for customer relation purposes and further screening of customer. [↑](#footnote-ref-7)