



POLICIES & PROCEDURES

Created by: Edward Dana

Employees **MUST** Log-in Super Stop
Online Training Portal at
www.SuperStop.us
At least once a month

Amended reflecting NOT offering

Money Transfer services August, 2011



Reviewed: Feb, 5th. 2014 Cash limits, Customer Privacy Additions & Review of Check Cashing AML

Reviewed: May, 22nd. 2013 Customer Privacy Additions & Review of Check Cashing AML, Cash limits

Reviewed: Jan, 13th. 2012 Customer Privacy Additions & Review of Check Cashing AML

Reviewed: August 1st. 2011 Not offering Money Transfer Services. Cancelled Western Union

Reviewed: July 1st. 2011

INTERNAL CONTROL GUIDE

CASH COLLECTIONS



INTRODUCTION

Cash is the most liquid of assets and is susceptible to loss if not properly controlled. Therefore, it is extremely important all departments handling cash implement and adhere to strong internal controls. **For the purposes of this guide, “cash” includes coins, Currency, checks, money orders, internal charges and credit card transactions.**

This Internal Control Guide provides guidance to Super Stop employees with regard to safeguarding cash. Please use this guide to develop cash handling procedures in our business.

Super Stop Employees MUST work on registers using their designated Log-in Credentials

OVERVIEW OF CASH HANDLING

The Compliance Officer or any of his administrative appointees is responsible for monitoring, processing and recording the collection of funds that come into Super Stop Market

Collections of funds at Super Stop Market are monitored, processed, and manager should distribute and deposit funds to the bank, as appropriate, in the course of normal operations. All employees collecting cash should ensure proper controls are in place to safeguard collections until final bank deposit.

All clerks collecting funds may be subject to periodic, unannounced audits and check-ups by the officers, managers or administrators.

In addition to collections, cash may be present in store for use as a change fund, check cashing funds or petty cash fund. A change fund earmarks an amount of cash to provide change for customers who make purchases from the store. A petty cash fund earmarks an amount of cash to be used by the store clerk to handle small, miscellaneous emergency purchases. In some cases the petty cash purchases would be paid by the clerk using his register cash sales if petty cash was not available. Clerk MUST record all pay outs on his final closing.

SEPARATION OF CASH HANDLING DUTIES

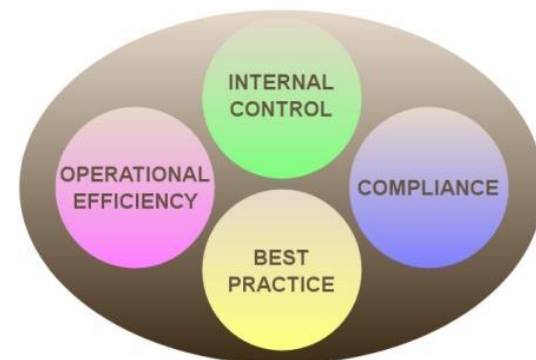
Cash handling duties can be divided into three stages: receiving, depositing, and reconciling. Ideally, all three stages might be performed by different individuals.



RECOMMENDED CONTROLS – RECEIVING CASH

In case of Receiving Checks and Money Orders

- All checks and money orders should be made payable to “Super Stop Market.”
- All checks should be restrictively endorsed at the time of receipt with “For Deposit Only,” along with the store name “Super Stop Market.”
- Payroll checks are cashed according to our check cashing system in place and clerk will be subject to pay for returned checks clerk cashed without following our check cashing system procedures.
- Prove of identity is required when processing a credit card transaction.
- Cash drawers, complete with a change fund, will always be fully prepared and secured.
- Change funds are not to be used by any employee for personal purposes.
- If a Super Stop employee is confronted with an armed assailant, or someone who proclaims to be armed, they will not resist and hand over all monies.
- It is critical to make cash drops into the safe when cash exceed more than \$1500.00 in one register.
- The numeric amount of the check must agree with the written amount.
- Checks must have the current date (no postdated checks).
- Change should never be given for a check over the amount due.
- If possible, each cashier should start his/her shift with new beginning cash balance and his/her own cash drawer. If a register must be shared, it must have sufficient controls to allow collections to be attributed to individual cashiers (e.g., separate user IDs and passwords to access the register).
- Cash register entries should be made at the time of the transaction, and the payer should be given a cash register receipt.
- Each cashier should balance his/her register activity at the end of the business shift.
- Store manager or a designated individual must verify daily that the cash received by clerk matches the total cash received in our POS database.
- All voids and refunds should be reviewed and approved by management and should be documented Safeguarding Handling and Storage of Cash
- All sales MUST be processed through the store registers.
- The customer should be given a copy of the receipt at the time of purchase if requested.
- You should never leave sales cash in an open unsecure area to customers all sales should be held in a secure manner until deposited. This may be accomplished by such means as a fireproof safe, a desk drawer, or other locked device.
- Access to secure locations via keys or combinations should be limited to authorize individuals only.
- Sales should be handled by employees as fast and as safe as possible.
- If cash is transferred to another clerk or employee, accountability procedures should be followed.



RECOMMENDED CONTROLS – DEPOSITING CASH

- All sales should finally be deposited into company bank account
- All deposits remitted to bank must be accompanied by a completed register ZZ closing Report/Receipts Voucher (sales Report). The sales Report must identify the source of the funds.
- All supporting documentation, including daily cashier reports, a daily summation of receipts, ATM machine cash and bank deposit slips should be included in the final report.
- Persons collecting and recording funds should not prepare deposits.
- Deposits must be made in a timely manner, with as little cash as possible being kept in store and manager should make daily deposits.
- When cash is deposited or when large sums of cash are on hand, departments are encouraged to ask for a police escort.



RECOMMENDED CONTROLS – RECONCILING CASH-RELATED ACTIVITY

- Reconciliations should be completed by the manager or a designated personnel the compliance officer should review the reconciliation process.
- Daily reconciliations should be performed by a specified individual, comparing the following:
- the cash receipt records (e.g., cash register balancing records, receipts, and cash drops) the completed sales Report
- Daily money orders review should be performed by the compliance officer or store manager to look for suspicious activities by looking over purchases made at the same time.
- All differences should be documented and resolved promptly.

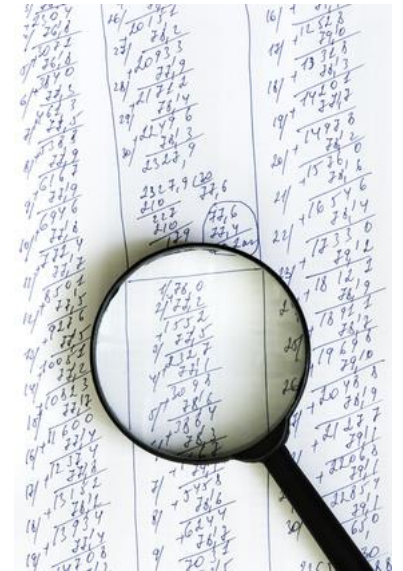
CASH HANDELING

RESOURCES

Company Compliance Officer: EDWARD DANA

If you have questions regarding cash handling procedures, you may ask:

- Edward Dana (502) 387-6133
- Ali Dana
- Melissa Dana



Cash Deposits and Reconciliation

PURPOSE

In order to maintain adequate internal controls, cash deposits and reconciliation submissions must be made on a daily basis if possible. The cash deposit must be placed in a blue bag and taken to the bank daily on working business days.

RESPONSIBILITY:

Store Manager → Edward Dana or Irina Khramova

ACTION


1. Prepares daily cash deposit to include cash and checks. Prepares Super Stop deposit slip.
2. The reconciler places the clerk receipt copies, credit card receipts and batch settlement, and reconciliation form into file.
3. The reconciler takes the deposit to the bank **or** places the deposit bag in a secured area until it's taken to the bank.

**ALL CASH TRANSACTIONS
MUST BE RECORDED,
DOCUMENTED AND FILED**

Super Stop must renew its Money Services Business license every 2 years.



Cash Drawer Procedures

| | | | | | | | | | | | | | | | |
|---------------------|--|---------------------|--------|--------------------|--------|------------------|---------|---------------------|---------|------|---------|-------|---------|------|---------|
| Purpose | <p>The Cash Drawer is defined as the working cash used in each cash drawer.</p> <ol style="list-style-type: none"> i. Check cashing or petty cash cannot be kept in the Cash Drawer. ii. Customer service requests for parking and telephone change and petty cash needs are acceptable uses of the Cash Drawer. | | | | | | | | | | | | | | |
| Policy | <p>RESPONSIBILITY Store Manager</p> <p><i>ACTION</i></p> <ol style="list-style-type: none"> 1. Each drawer should be setup with an initial \$146.00. The break down should follow a pattern similar to the one given below. This is only a guideline and, as drawers run low of a certain denomination, that denomination will need to be replenished. <table style="margin-left: 100px; border: none;"> <tr> <td style="padding-right: 20px;">Pennies (two rolls)</td> <td style="text-align: right;">\$2.00</td> </tr> <tr> <td>Nickels (one roll)</td> <td style="text-align: right;">\$4.00</td> </tr> <tr> <td>Dimes (one roll)</td> <td style="text-align: right;">\$10.00</td> </tr> <tr> <td>Quarters (one roll)</td> <td style="text-align: right;">\$20.00</td> </tr> <tr> <td>Ones</td> <td style="text-align: right;">\$30.00</td> </tr> <tr> <td>Fives</td> <td style="text-align: right;">\$30.00</td> </tr> <tr> <td>Tens</td> <td style="text-align: right;">\$50.00</td> </tr> </table>  <ol style="list-style-type: none"> 2. As cash is given out for change and taken in for payment, the composition of the drawer will change. Observe which denomination has the most activity and order more of that denomination than other currency and coin that is not given out as much. An example is that quarters are used more frequently than one dollar bills. Dollar bills should be taken in exchange for quarters in this example, so less one dollar bills are needed and more quarters would be kept on hand. 3. As additional change is needed to replenish the change fund the manager will take it out of our company bank account 4. For internal control purposes it is recommended that a drawer be provided to each employee handling cash. 5. Loan to a register will be given to handle store check cashing business <p>RESPONSIBILITY Manager</p> <ol style="list-style-type: none"> 1. Unannounced periodic cash counts of the cash drawers will take place on an ongoing basis. <p>RESPONSIBILITY Cashier</p> <ul style="list-style-type: none"> • Change may be given to customers for non-payment type exchanges; this might include change for parking and telephone use. When change is provided to the customers, the cashier should ensure that equal amounts are exchanged. | Pennies (two rolls) | \$2.00 | Nickels (one roll) | \$4.00 | Dimes (one roll) | \$10.00 | Quarters (one roll) | \$20.00 | Ones | \$30.00 | Fives | \$30.00 | Tens | \$50.00 |
| Pennies (two rolls) | \$2.00 | | | | | | | | | | | | | | |
| Nickels (one roll) | \$4.00 | | | | | | | | | | | | | | |
| Dimes (one roll) | \$10.00 | | | | | | | | | | | | | | |
| Quarters (one roll) | \$20.00 | | | | | | | | | | | | | | |
| Ones | \$30.00 | | | | | | | | | | | | | | |
| Fives | \$30.00 | | | | | | | | | | | | | | |
| Tens | \$50.00 | | | | | | | | | | | | | | |

Processing Credit Card Payments

PURPOSE Store Clerk is responsible to accommodate credit card transactions.

RESPONSIBILITY

Clerk

ACTION

1. **Receive request to make payment by credit card.**
2. Swipe credit card (VISA, MasterCard, Discover, or American Express) through credit card terminal (OMNI Machine or on-line process).
3. Enter amount of payment on credit card terminal and press enter.
4. Credit card terminal prints authorization number on sales draft.
5. Ask cardholder to sign sales draft.
6. If the credit card transaction cannot be completed due to an error message on the credit card terminal (such as an over limit, fraudulent card, or any other reason) return the card to the customer and ask for another form of payment.
7. Clerk must include a sales receipt for any credit card transaction of \$50 dollars or more and should be dropped at the end of his/her shift for store manager review.



Proper handling of credit card information for Compliance

Responsibility

Anyone Accepting Credit Card Payment

Due to increased global threat of identity theft and compliance requirements from our financial institutions and merchant service providers, increased diligence is required for all service sites processing credit card payments or refunds. The following applies to sensitive credit card information:

- a.) The cardholder and account information (name, address, full account number, and expiration date or 3-digit security code on the back of the card) must not be retained once the card processing is complete.
 - b.) Examples of improper retention include, maintaining electronic spreadsheets or databases with such information listed, keeping hard-copy file folders with this data in a written format, or maintaining such information in e-mails.
 - c.) If such information is presented to you (i.e. a third party written authorization or is written down as a reference to complete the transaction), it must be promptly and safely destroyed using a shredder in manager office.
2. Treasury and CFS may, as part of ongoing compliance requirements, conduct random service site procedure evaluations. Site managers may also periodically be requested to complete a compliance questionnaire for internal control purposes.

Voiding Credit Card Transactions

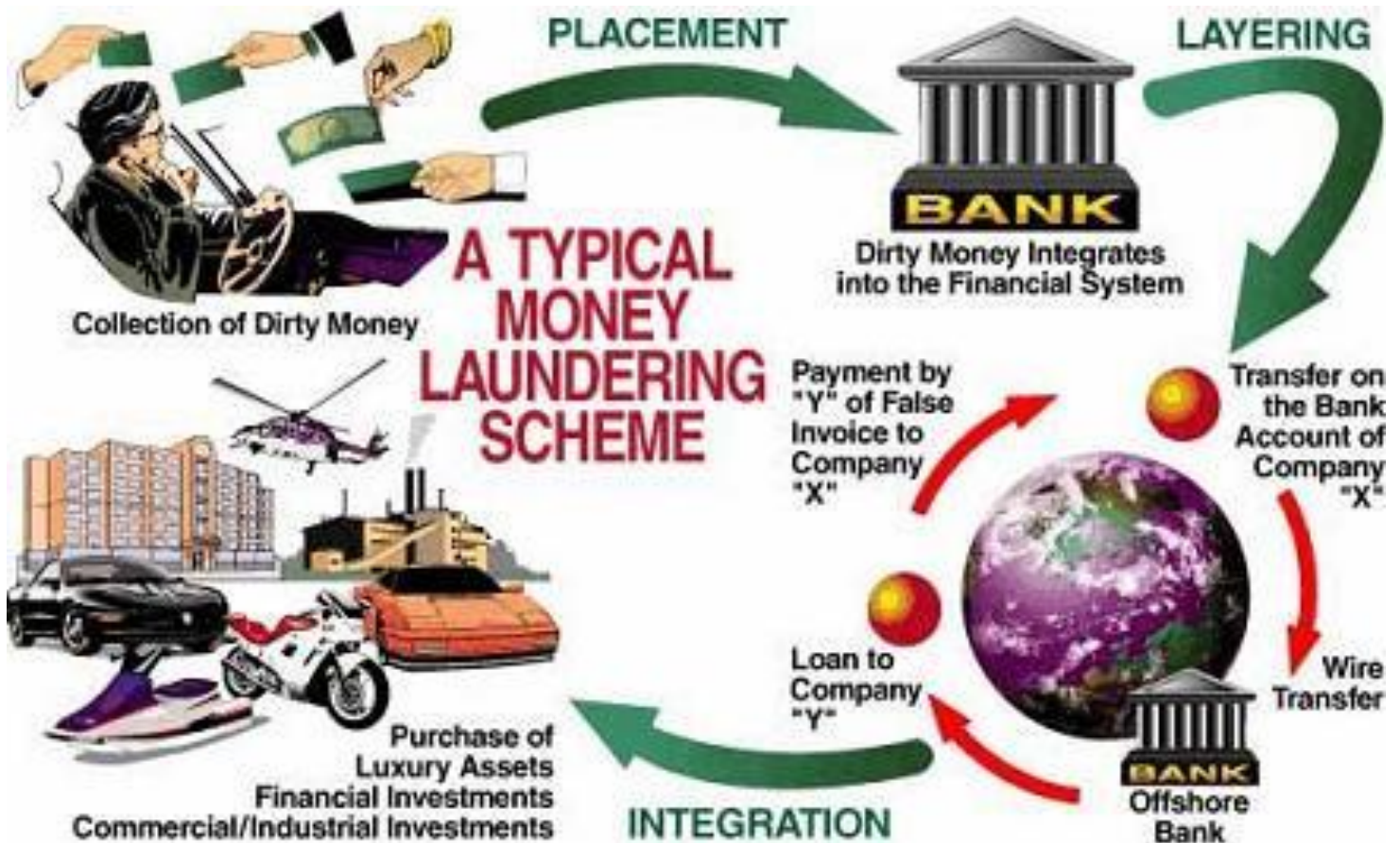
PURPOSE Follow this procedure to cancel a credit card transaction if an error is made in the amount of the transaction, and the credit card machine has not been batch settled.

RESPONSIBILITY

Clerk

ACTION

1. **Press void on the credit card terminal**
2. To void a transaction by the ticket number, press 1 and then press enter/yes.
3. Enter the ticket number of transaction and press enter/yes.
4. If the ticket number and amount of transaction is correct, press enter/yes.
 1. A voided receipt will print. Circle the word "VOID" and keep with credit card transactions until settlement procedure is performed.
 2. If ticket number and/or amount of a transaction are incorrect, press clear/no and start again.



Check Cashing Policies & Procedures

Stop Check Fraud

Non-Sufficient Funds Policy and Procedure

PURPOSE This procedure outlines the steps taken when cashed checks are returned by the bank for NON-sufficient funds/stop payment/account closed (NSF). Returned checks require a sequence of actions.

RESPONSIBILITY

Staff

ACTION

1. Receive returned check then print a transaction report from the check cashing computer.
2. Review the endorsement stamp and receipt number on the back of the check. Identify which clerk cashed the check.
3. Cashier or manager should call customer and investigate why check was returned.
4. Call company, organization or government department that issued the check and investigate why check was returned.
5. Always talk to customer about their legal obligation and the consequences they face if they don't cooperate and help us in getting our money back.



Follow Store Procedures

Super Stop provides check-cashing service to customers that have a valid Kentucky driver license or a valid Kentucky identification card.

Daily Check Cashing Limits

The check cashing limit is a minimum of \$5 up to a maximum of \$999.00. Checks \$1000 and over will **require a manager presence and approval** to cash.

Suspension of Check Cashing Privilege

Super Stop Market reserves the right to suspend or terminate a customer check cashing privileges for returned checks or other financial reasons. If the returned checks are the result of a bank or a company error and were reimbursed, the privilege will be reinstated.

Collection of Returned Checks

A \$35 fee will be charged for each returned check. The customer will be notified by phone and required to respond within three (3) business days. Failure to respond to this notice will result in a legal action. Follow the collection of a returned check procedure.

SUPER STOP IS A REGISTERED MONEY SERVICE BUSINESS

Allowable Check Cashing

- Payroll checks.
- Government checks.
- Insurance checks.
- Money Orders
- Income tax refund checks

Fees for Check Cashing

Super Stop fee will be based on the following schedule:

| Check amount | Fee |
|--------------------------|---------------------------|
| \$100.00 | 2% |
| \$100 → \$200 | 2% |
| \$200 → \$300 | 2% |
| \$300 + | 2.5% |
| Periodic Sales discounts | We cash checks for change |



Limitation and Requirements For Check Cashing

Customers: a valid official picture ID (i.e. valid Driver's License, Government issued picture ID).

All Others: Valid green Card alien resident card or passport.

Information required every time we cash a check

- Signature endorsement on back of check
- Current address and telephone number and if it doesn't match the customer information in our database please correct it
- You must update customer phone number in system every time they cash a check.

Third-Party Checks

A third-party check is a check that is written to one person, and then signed over to another person.

SUPER STOP DOES NOT ACCEPT THIRD-PARTY CHECKS

Handwritten Checks

Do not accept checks that are not typed or computer generated. Handwritten checks could be stolen with a forged signature.

Check Number Limit

The number of checks each customer can cash per month is 4 checks.



Check Cashing System

Super Stop check cashing system is innovation database software to help and speed the check cashing process. It is very important that all customer information in our database is correct and updated every time the customer return to our store.

Fingerprint

Super Stop requires the customer to include a finger or thumb print in our database along with the ID and signature endorsement. If the check clears, there is no issue. However, if the check is returned for insufficient funds or as a stolen or forged check, the fingerprint can be cross-checked for criminal activity. You can include this as a check cashing procedure.

Taking a picture of the Customer

Super Stop requires taking a current picture to our check cashing returned customers.



Check Fraud Scenarios

When a check is returned and we failed to communicate or get reimbursed for our loss by the customer or the check issuer the store manager or clerk should proceed with the following:

- Store manager or clerk must call Louisville Check Fraud unit at: **(502) XXX-XXXX**
- Prepare 2 complete check transaction reports from our check cashing system including all customer and check information. A copy goes to the Fraud unit and the second for our internal filling.

Check Drops and deposits

When a check is cashed it will have to be dropped into our safe immediately as soon as possible and after cash reconciliation all checks **MUST** be deposited in the bank account to get credited as fast as possible.

CTR Preparations

When to file a CTR:

- If a customer bring a check that is more than \$10,000 or more.
- If a customer bring 2 checks totaling \$10,000 or more.



Cashing Money Orders

When to cash a money order:

- Money order **MUST** be blank and not filled out
- Money order **MUST** have the stub that is attached to it.
- Customer must have valid identification.
- Money orders are not processed into our check cashing system because they are not payroll checks.
- Do not cash money orders exceeding \$500.00 dollars.



Employee Responsibility for returned checks

When a check is returned for any reason due to clerk error Super Stop reserve the right to charge clerk for the full amount of the check including any charges that might occur by our financial institution

RECORD DISPOSAL REQUIREMENTS UNDER THE BUSINESS ADMINISTRATION ACT

All Employees must understand the proper disposal of Super Stop records that contain the following:

- Sensitive information about a customer's medical condition
- Certain financial data relating to a customer's account or transaction with Super Stop
- Data provided by a customer to Super Stop upon any financial transaction.
- Data about a customer's federal, state, or local tax return.

Once such records are no longer needed, Super Stop must do one of the following before discarding them:

- A. Shred the record
- B. Erase the personal information contained in the record
- C. Modify the record so that the personal information is unreadable
- D. Take actions that will ensure that no unauthorized person will have access to the personal information contained in the records.

Improper disposal of records containing personal information may result in losing you job and serious legal actions.

Check Cashing Responsibilities

DO NOT Cash Checks more than \$500 without manager APPROVAL

- Report fraudulent or forged checks.
- Super Stop will maintain digital logs of checks cashed.
- Maintain a daily reconciliation of cash.
- Report any illegal activities immediately.
- Post fees charged for cashing checks.
- Post the license in plain view.



EBT Food Stamp SNAP requirement for business accepting EBT cards program.

What foods can customers buy with SNAP food stamps?

- Customers can use SNAP food stamps to buy any food item except food that is hot when sold, or food that is sold to be eaten in the store like restaurant food. Eligible food items include:
 - any food products or ingredients used to prepare meals at home
 - cold prepared sandwiches, salads, and other deli items
 - ethnic and health foods
 - snack foods, candy, soda, and ice
- Customers can use SNAP food stamps to buy seeds or plants that they will grow to produce food for their household.
- Customers cannot use SNAP food stamps to buy non-food items like alcoholic beverages, cigarettes, vitamins or medicines, pet foods, soap, cosmetics, laundry products, paper goods, or other household products.



ACCESS SERVICES TRAINING PORTAL ON OUR WEBSITE PERIODICALLY

What rules do I have to follow?

Super Stop management will explain the rules employees must follow for the SNAP Food Stamp Program. They will also explain the penalties for not following the rules. Some of the most important rules are:

- You can only accept SNAP food stamps for eligible food items.
- You cannot charge sales tax on any items bought with SNAP food stamps.
- You cannot accept SNAP food stamps as payment on credit accounts. Your food stamp customers must pay for their purchases at the time of sale. You cannot give them credit and let them pay you back with SNAP food stamps at a later date.
- You cannot give cash in exchange for SNAP food stamps.
- You cannot give cash change for SNAP purchases. The amount charged to the customer's EBT account must be the exact amount of the food purchase.
- You cannot give cash refunds for food bought with SNAP food stamps. Refunds must go to the customer's EBT account.
- You cannot process a SNAP purchase unless the customer has the EBT card and PIN.
- You must treat SNAP food stamp customers and other customers the same. For example, you cannot have a special line for SNAP food stamp customers, or charge them higher prices, or require a minimum purchase.

**You must follow all of the SNAP Food Stamp Program rules and regulations. If you do not follow the rules, you can lose your job.
You may also be subject to a legal action.**

Money Orders

Purpose:

Money Order Record – Consumer Identification and Recordkeeping Requirements for Money Orders

To establish policies and procedures for the consistent review, verification, and recording of consumer identification and transaction information for money order purchases of \$3,000 or more (inclusive of fees) by or on behalf of a single consumer in any one day.

Procedures:

Consumer Identification Requirements for Money Orders -- \$3,000 or more

1. For all Money Order purchases of \$3,000 or more (inclusive of fees), whether purchased singly or in the aggregate, by or on behalf of a consumer in any one day, employees must obtain and record the following consumer and transaction information.

2. Employees are required to review an acceptable form of consumer identification and ensure that the identification:

- Is currently valid (i.e., has not expired)
- Is government issued
- Contains a photograph of the consumer
- Contains the consumer's name
- Contains the consumer's address (preferred)

3. Employees must determine that the form of identification is acceptable by Super Stop policy. Examples of acceptable forms of identification include the following:

- Driver's License
- Passport
- US Permanent Resident Card (green card)
- Military I.D. Card
- Mexican Consulate Issued Matricula Card

4. Employees must look at and handle the consumer's ID to verify the consumer's identity and the ID's authenticity. If an ID is not provided, does not match the consumer, or appears to be fake the employee must refuse the transaction.

5. Employees must obtain and record the following information on the Money Order Record:

- Purchase Date
- Total number of Money Orders sold

Our Services

SUPER STOP Services

1) Money Orders



3) Check Cashing

4) Bill Payment

5) Kentucky Lottery

6) ATM Machine

7) Phone Cards



- Money Orders → Global Express
- Bill Payment → Global Express
- Kentucky Lottery → Kentucky Lottery
- ATM Machine → CPR Financial
- Phone Cards → Different Distributors
- Check Cashing



Anti-Money Laundering Policy Statement & Program Procedures

Compliance and Supervisory Procedures for

SUPER STOP

7303 Preston Hwy. Louisville, KY 40219

I. Company Anti-Money Laundering Policy Statement

It is the policy of Super Stop to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorists or criminal activity.

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origin of criminally derived proceeds so that the unlawful proceeds appear to have derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

- **Placement:** Cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.
- **Layering:** Funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.
- **Integration:** Funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal the origin or intended use of the funds, which will later be used for criminal purposes.

II. AML Compliance Officer Designation and Duties

As required under the USA Patriot Act of 2001 (PATRIOT Act), **Super Stop designates Edward Dana as the Anti-Money Laundering Program Compliance Officer, with full responsibility for the Company's anti-money laundering (AML) program.** Super Stop will insure compliance of AML at all times and will train its employees to fight and report crimes. Super Stop will insure proper handle of all cash received from its customers thru the appropriate channels counted for until it is safely deposited into the company's bank. The AML Compliance Officer will also ensure that proper AML records are kept. When warranted, the AML Compliance Officer will ensure Suspicious Activity Reports (see Appendix Form TD F90-22.56) are filed with the Financial Crimes Enforcement Network (FinCEN) or the Company's designated self-regulatory agency (DSRO).

III. Sharing AML Information with Federal Law Enforcement Agencies and Other Financial Institutions

Under the U.S. Treasury's final regulations (published in the Federal Register on September 26, 2002), Super Stop will respond to any FinCEN request about accounts or transactions by immediately searching our records to determine whether we maintain or have maintained any account for, or have engaged in any transaction with, each individual, entity, or organization named in FinCEN's request. Upon receiving an information request, the AMLCO is to be responsible regarding the request and similar requests in the future. Unless otherwise stated in FinCEN's request, we are required to search current accounts and transactions, accounts maintained by a named suspect during the preceding 12 months, and transactions conducted by or on behalf of or with a named subject during the preceding six months. If we find a match, we will report it to FinCEN by completing FinCEN's subject information form in a timely manner. If we search our records and do not uncover a matching account or transaction, then we will not reply as allowed under Section 314(a) of the PATRIOT Act.



We will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request. We will maintain procedures to protect the security and confidentiality of requests from FinCEN, as required by Section 501 of the Gramm-Leach-Bliley Act. We will direct any questions we have about the request to the requesting Federal law enforcement agency as designated in the 314(a) request.

Unless otherwise stated in the information request, we will not be required to treat the information request as continuing in nature, and we will not be required to treat the request as a list for purposes of the customer identification and verification requirements. We will not use information provided to FinCEN for any purpose other than (1) to report to FinCEN as required under Section 314 of the PATRIOT Act; (2) to determine whether to establish or maintain an account, or to engage in a transaction; or (3) to assist the Company in complying with any requirement of Section 314 of the PATRIOT Act.

A. Sharing Information with Other Financial Institutions

Super Stop will share information about those suspected of terrorist financing and money laundering with other financial institutions for the purposes of identifying and reporting activities that may involve terrorist acts or money laundering activities and to determine whether to establish or maintain an account or engage in a transaction. We will file an initial notice with FinCEN before any sharing occurs and annual notices afterwards. We will use the notice form found at http://www.fincen.gov/fi_infoappb.html or use a paper notification mailed to FinCEN, P.O. Box 39, Mail Stop 100, Vienna, VA 22183. Before we share information with another financial institution, we will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. We understand that this requirement applies even with respect to financial institutions with whom we are affiliated, and so we will obtain the requisite notices from affiliates and follow all required procedures.

Super Stop will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, including segregating it from the firm's other books and records.

IV. Checking the Office of Foreign Assets Control (OFAC) Lists

Before engaging in any money service activity (including but not limited to check cashing, money orders and wire transfers) which potentially may involve money laundering, and on an ongoing basis, we will check to ensure that a customer does not appear on the Treasury's OFAC "Specifically Designated Nationals and Blocked Persons" List, SDN List, and is not from, or engaging in transactions with people or entities from, embargoed countries and regions listed on the OFAC website (see www.treas.gov/offices/enforcement/ofac/sdn/index.html).

Because the OFAC Website is updated frequently, we will consult the list on a regular basis and subscribe to receive updates when they occur. We may, if necessary, access these lists through various software programs to ensure speed and accuracy. We will also review existing accounts against these lists when they are updated and we will document our review.

In the event that we determine a customer, or someone with or for whom the customer is transacting, is on the SDN List or is from or engaging in transactions with a person or entity located in an embargoed country or region, we will reject the transaction and/or block the customer's assets and file a blocked assets and/or rejected transaction form with OFAC. We may also call the OFAC Hotline at **1-800-540-6322**.



V. Customer Identification and Verification

We have established, documented, and maintained a written Customer Identification Program (or CIP). We will collect certain minimum customer identification information from each customer who engages in any money service activity with the Company; utilize risk-based measures to verify the identity of each customer who engages in any money service activity; record customer identification information and the verification methods and results; provide notice to customers that we will seek identification information and compare customer identification information with government-provided lists of suspected terrorists as mentioned above in Section III.

A. Required Customer Information

Prior to cashing a check or engaging in any money service activity which potentially may involve money laundering, we will collect the following information for all customers: the name; an address, (which will be a residential or business street address for an individual), an Army Post Office ("APO") or Fleet Post Office ("FPO") number; an identification number, which will be a taxpayer identification number (for U.S. persons) or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard (for non-

U.S. persons). We will refuse any money service transaction in the event that a customer has applied for, but has not received a taxpayer identification number and cannot prove his/her identity to the satisfaction of the AMLCO.

B. Customers Who Refuse To Provide Information

If a potential or existing customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, Super Stop will not conduct any further money service transactions with that entity. In either case, our AML Compliance Officer will be notified so that we can determine whether we should report the situation to FinCEN (i.e., file a Form SAR-MSB).

Super Stop Employees MUST Notify the compliance officer of any Suspicious Activities Immediately

C. Verification of Information

Based on the risk, and to the extent reasonable and practicable, we will ensure that we have a reasonable belief that we know the true identity of our customers by using risk-based procedures to verify and document the accuracy of the information we get about our customers. In verifying customer identity, we will analyze any logical inconsistencies in the information we obtain.

We will verify customer identity through documentary evidence, non-documentary evidence, or both. We will use documents to verify customer identity when appropriate documents are available. In light of the increased instances of identity fraud, we will supplement the use of documentary evidence by using the non-documentary means described below whenever possible. We may also use such non-documentary means, after using documentary evidence, if we are still uncertain about whether we know the true identity of the customer. In analyzing the verification information, we will consider whether there is a logical consistency among the identifying information provided, such as the customer's name, street address, zip code, telephone number (if provided), date of birth, and social security number. Appropriate documents for verifying the identity of customers include, but are not limited to, the following:

- For an individual, an unexpired government-issued identification evidencing nationality, residence, and bearing a photograph or similar safeguard, such as a driver's license or passport; and
- For an entity, other than an individual, documents showing the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or a trust instrument.

We understand that we are not required to take steps to determine whether the document that the customer has provided to us for identity verification has been validly issued and that we may rely on a government-issued identification as verification of a customer's identity. However, if we note that the document shows some obvious form of fraud, we must consider that factor in determining whether we can form a reasonable belief that we know the customer's true identity.

We may use any or all of following non-documentary methods of verifying identity:

- Contacting a customer;
- Independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, employer or other source;
- Checking references with financial institutions;

We will use non-documentary methods of verification in the following situations:

- 1) When the customer is unable to present an unexpired government-issued identification document with a photograph or other similar safeguard;
- 2) When the Company is unfamiliar with the documents the customer presents for identification verification;
- 3) When there are other circumstances that increase the risk that the Company will be unable to verify the true identity of the customer through documentary means.

We will verify the information within a reasonable time before a transaction is completed. Depending on the nature of the requested transaction, we may refuse to complete a transaction before we have verified the information, or in some instances when we need more time, we may, pending verification, restrict the types of transactions or dollar amount of transactions. If we find suspicious information that indicates possible money laundering or terrorist financing activity, we will, after internal consultation with the firm's AML compliance officer, file a SAR-MSB in accordance with applicable law and regulation.

D. Lack of Verification

When we cannot form a reasonable belief that we know the true identity of a customer, we will do the following:

- I. Not perform any money service transaction;
- II. Impose terms under which a customer may conduct transactions while we attempt to verify the customer's identity;
- III. File a SAR-MSB in accordance with applicable law and regulation.

**(SAR) SUSPICIOUS ACTIVITY REPORT MUST BE FILED IN
ACCORDANCE WITH THE LAW**

E. Recordkeeping

We will document our verification, including all identifying information provided by a customer, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. We will keep records containing a description of any document that we relied on to verify a customer's identity, noting the type of document, any identification number contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, we will retain documents that describe the methods and the results of any measures we took to verify the identity of a customer. We will maintain records of all identification information for five years after the account has been closed and readily accessible for the first two years. We will retain records made about verification of the customer's identity for five years after the record is made.

F. Comparison with Government Provided Lists of Terrorists and Other Criminals

The Company may receive notice that a Federal government agency has issued a list of known or suspected terrorists. Within a reasonable period of time after an account is opened or transaction is completed (or earlier, if required by another Federal law or regulation or Federal directive issued in connection with an applicable list), we will determine whether a customer appears on any such list of known or suspected terrorists or terrorist organizations issued by any Federal government agency and designated as such by Treasury in consultation with the Federal functional regulators.

- ✦ We will follow all Federal directives issued in connection with such lists.
- ✦ We will continue to comply with Treasury's OFAC rules prohibiting transactions with certain foreign countries or their nationals as mentioned in Section III.

G. Notice to Customers

We will provide notice to customers that Super Stop is requesting information from them to verify their identities, as required by Federal law. We will give notice to customers regarding the policy either verbally or as a plainly posted notice such as:

To help the government fight the funding of terrorism and money laundering activities, Federal law requires us to obtain, verify, and record information that identifies each person who cashes checks, wire funds or engages in other financial services with this establishment. We will ask for your name, address and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documents.

H. Reliance on another Financial Institution for Identity Verification

Under the following circumstances we may rely on the performance by another financial institution of some or all of the elements of our customer identification program with respect to any customer that is engaging in a money service transaction with the other financial institution to provide or engage in services, dealings, or other financial transactions:

- ❖ When such reliance is reasonable under the circumstances;
- ❖ When the other financial institution is subject to a rule implementing the anti-money laundering compliance program requirements of 31 U.S.C. 5318(h), and is regulated by a Federal functional regulator.

VI. Foreign Correspondent Accounts and Foreign Shell Banks

It is our policy that Super Stop will not engage in any money service transactions when we have a reasonable cause to believe a foreign bank or foreign financial institution is involved in any way.

VII. Monitoring Accounts for Suspicious Activity

We will manually monitor a sufficient amount of money service activity to permit identification of patterns of unusual size, volume, pattern or type of transactions, geographic factors such as whether jurisdictions designated as "non-cooperative" are involved, or any of the "red flags" identified in Section VII. A. 1 below. The AML Compliance Officer will be responsible for this monitoring, will document when and how it is carried out, and will report suspicious activities to the appropriate authorities. Among the information we will use to determine whether to file a Form SAR-MSB are exception reports that include transaction size, location, type, number, and nature of the activity. We will create employee guidelines with examples of suspicious money laundering activity and lists of high-risk clients whose accounts may warrant further scrutiny. Our AML Compliance Officer will conduct an appropriate investigation before a SAR is filed.



A. Emergency Notification to the Government

When conducting due diligence we will immediately call Federal law enforcement when necessary, and especially in these emergencies: a legal or beneficial account holder or person with whom the account holder is engaged in a transaction is listed on or located in a country or region listed on the OFAC list, an account is held by an entity that is owned or controlled by a person or entity listed on the OFAC list, a customer tries to use bribery, coercion, or similar means to open an account or carry out a suspicious activity, we have reason to believe the customer is trying to move illicit cash out of the government's reach, or we have reason to believe the customer is about to use the funds to further an act of terrorism. We may contact the OFAC via its hotline at 1-800-540-6322 or electronically through its website at www.treas.gov/offices/enforcement/ofac.

1. Detecting Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

- The customer exhibits unusual concern about the Company's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or documents.
- The customer wishes to engage in a transaction that lack business sense or is inconsistent with the customer's stated business.
- The information provided by the customer that identifies a legitimate source for funds is false, misleading, or substantially incorrect.
- Upon request, the customer refuses to identify or fails to indicate any legitimate source for his or her funds and other assets.
- The customer (or a person publicly associated with the customer) has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations.
- The customer exhibits a lack of concern regarding transaction costs.
- The customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity.
- The customer has difficulty describing the nature of his or her business.
- The customer attempts to conduct frequent or large transactions, or asks for exemptions from the Company's AML policies.
- The customer engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the \$10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds.
- For no apparent reason, the customer has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers.
- The customer is from, or has accounts in, a country identified as a non-cooperative country or territory by the FATF.
- The customer has unexplained or sudden extensive money service activity, especially when they that had little or no previous activity.
- The customer has a large number of wire transfers to unrelated third parties inconsistent with the customer's legitimate business purpose.
- The customer has financial activity with no apparent business purpose to or from a country identified as money laundering risk or a bank secrecy haven.
- The customer makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose.
- The customer requests that a transaction be processed to avoid the Company's normal documentation requirements.
- The customer uses multiple accounts, or maintains accounts in the names of family members or corporate entities, with no apparent purpose.
- The customer has inflows of funds or other assets well beyond the known income or resources of the customer.

2. Responding to Red Flags and Suspicious Activity

When a member of the Company detects any red flag he or she will investigate further under the direction of the AML Compliance Officer. This may include gathering additional information internally or from third-party sources, contacting the government, freezing the account, or filing a Form SAR-MSB.

VIII. Suspicious Transactions and BSA Reporting

A. Filing a Form SAR-MSB

We will file Form SAR-MSBs for any activity (including deposits and transfers) conducted or attempted through our Company involving (or in the aggregate) \$2,000 or more of funds or assets where we know, suspect, or have reason to suspect:

- 1) The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation,
- 2) The transaction is designed, whether through structuring or otherwise, to evade the any requirements of the BSA regulations,
- 3) The transaction has no business or apparent lawful purpose or is not the sort in which the customer would normally be expected to engage, and we know, after examining the background, possible purpose of the transaction and other facts, of no reasonable explanation for the transaction, or
- 4) The transaction involves the use of the Company to facilitate criminal activity.

We will not base our decision on whether to file a SAR-MSB solely on whether the transaction falls above a set threshold. We will file a SAR-MSB and notify law enforcement of all transactions that raise an identifiable suspicion of criminal, terrorist, or corrupt activities. In high-risk situations, we will notify the appropriate government agency immediately and will file a SAR-MSB with FinCEN.

We will report suspicious transactions by completing a SAR-MSB and we will collect and maintain supporting documentation as required by the BSA regulations. We will file a SAR-MSB no later than 30 calendar days after the date of the initial detection of the facts that constitute a basis for filing a SAR-MSB. If no suspect is identified on the date of initial detection, we may delay filing the SAR-MSB for an additional 30 calendar days pending identification of a suspect, but in no case, will the reporting be delayed more than 60 calendar days after the date of initial detection. We will retain copies of any SAR-MSB filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-MSB. We will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, or federal or state regulators, upon request.

We will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. We understand that anyone who is subpoenaed or required to disclose a SAR-MSB or the information contained in the SAR-MSB, except where disclosure is requested by FinCEN, or other appropriate law enforcement or regulatory agency or an SRO, will decline to produce to the SARMSB or to provide any information that would disclose that a SAR-MSB was prepared or filed. We will notify FinCEN of any such request and our response.

B. Currency Transaction Reports (CTR)

If we receive currency, we will file with FinCEN CTRs for transactions involving currency that exceed \$10,000. Multiple transactions will be treated as a single transaction if they total more than \$10,000 during any one business day. We will use the Form CTR at www.fincen.gov/fin104_ctr.pdf (see Appendix).

IX. AML Record Keeping

A. SAR-MSB Maintenance and Confidentiality

We will hold SAR-MSBs and any supporting documentation confidential. We will not inform anyone outside of a law enforcement or regulatory agency about a SAR-MSB. We will refuse any subpoena requests for SAR-MSBs or SAR-MSB information and immediately tell FinCEN of any such subpoena we receive. We will segregate SAR-MSB filings and copies of supporting documentation from other Company books and records to avoid disclosing SAR-MSB filings. Our AML Compliance Officer will handle all subpoenas or other requests for SAR-MSBs. We will share information with our bank about suspicious transactions in order to determine when a SAR-MSB should be filed – unless it would be inappropriate to do so under the circumstances, such as where we file a SAR-MSB concerning the bank or its employees.

B. Responsibility for AML Records and SAR Filing

Our AML Compliance Officer and his or her designee will be responsible to ensure that AML records are maintained properly and that any SARs are filed as required.

C. Records Required

As part of our AML program, Super Stop will create and maintain SAR-MSBs, and other relevant documentation on customer identity and verification (see Section IV above) and funds transfers and transmittals as well as any records related to customers listed on the OFAC list. We will maintain SAR-MSBs and their accompanying documentation for at least five years.

X. Bank / Company Relationship

We will work closely with our banking firm to detect money laundering. We will exchange information, records, data and exception reports as necessary to comply with AML laws. The appropriate notification forms can be found at www.fincen.gov/fi_infoappb.html. Generally we have agreed that the Company will monitor customer activity including proper customer identification information as required.

XI. Training Programs

We developed ongoing employee training under the leadership of the AML Compliance Officer. Our training will occur on at least an annual basis. Based on our firm's size, its customer base, and its resources we have determined that Exchange Analytics, Inc. will provide the training course to our staff. The course is administered online at https://www.xanalytics.com/aml/aml_frame.htm.

The training course offered by Exchange Analytics includes, at a minimum: how to identify red flags and signs of money laundering that arise during the course of the employees' duties; what to do once the risk is identified; what employees' roles are in the firm's compliance efforts and how to perform them; the Company's record retention policy; and the disciplinary consequences (including civil and criminal penalties) for non-compliance with the PATRIOT Act. The training program offered by Exchange Analytics, Inc. includes the maintenance of the records to show the persons trained, the dates of training, and the subject matter of their training.

Training, in lieu of the Exchange Analytics online course, will also include educational pamphlets, videos, intranet systems, in-person lectures, and explanatory memos as necessary.

We will review our operations to see if certain employees, such as those in compliance, margin, and corporate security, require specialized additional training. Our written procedures will be updated to reflect any such changes.

XII. Program to Test AML Program

Annual testing of our AML program will be performed either by EA Compliance, Inc. an independent third party which is primarily focused on PATRIOT Act compliance matters or other qualified independent third party or internally by a qualified member of Super Stop's staff. The annual testing will include an audit of our compliance with our AML program. The auditor will issue a report of the auditor's findings upon completion their audit to senior management. We will address each of the resulting recommendations.



XIII. Monitoring Employee Conduct and Accounts

We will subject employee money service transactions to the same AML procedures as customer accounts, under the supervision of the AML Compliance Officer. We will also review the AML performance of supervisors, as part of their annual performance review. The AML Compliance Officer's accounts will be reviewed by a qualified member of the Company staff.

XIV. Confidential Reporting of AML Non-Compliance

Employees will report any violations of the firm's AML compliance program to the AML Compliance Officer, unless the violations implicate the Compliance Officer, in which case the employee shall report to an appropriate member of senior management. Such reports will be confidential, and the employee will suffer no retaliation for making them.

XV. Additional Areas of Risk

The Company has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above and is continually working to improve its AML program.

XVI. Senior Manager Approval

I have approved this AML program as reasonably designed to achieve and monitor Super Stop's ongoing compliance with the requirements of the USA PATRIOT Act of 2001 and the implementing regulations under it.

Name: _____ Title: _____

Signed: _____ Date: _____



Customer Privacy Policy

SUPER STOP

7303 Preston Hwy. Louisville, KY 40219



SUPER STOP RECOGNIZES THE IMPORTANCE OF RESPECTING CUSTOMERS' RIGHT TO PRIVACY AND ADHERES TO THE FOLLOWING KEY PRINCIPLES:

- Super Stop is responsible for personal information under its control and has designated individuals to be accountable for the organization's compliance.
- The purposes for which personal information is collected will be identified at or before the time the information is collected.
- Knowledge and consent will be obtained for the collection, use, and disclosure of personal information, except where deemed inappropriate.
- The collection of personal information is limited to that which is related to the purposes identified by Super Stop.
- Personal information will not be used or disclosed for purposes other than those for which it was collected, except with the consent of the customer or as required by law.
- Reasonable efforts will be made to ensure that personal information is as accurate, complete, and up-to-date as is necessary for the purposes for which it is used.
- Personal information will be protected by reasonable security safeguards appropriate to the sensitivity of the personal information.
- Information is available to customers regarding Super Stop's policies and procedures relating to the management of personal information.
- Upon request, and within a reasonable period of time, a customer will be informed of the existence, use, and disclosure of his or her personal information and will be given access to that information. A customer is entitled to comment on the accuracy and completeness of his or her personal information, and have that information amended where appropriate.
- A customer can address a challenge concerning compliance with the above principles to Super Stop's designated Compliance Officer.

