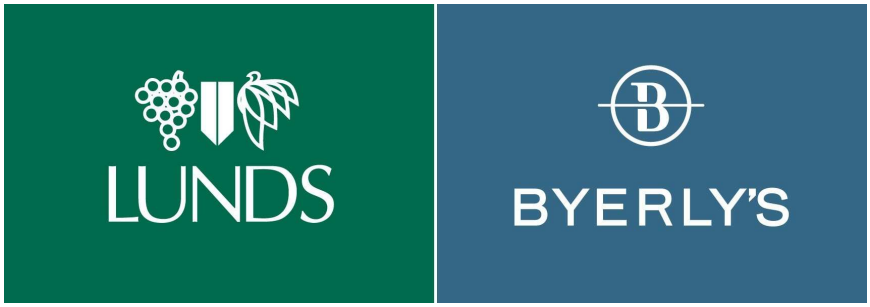

ANTI-MONEY LAUNDERING POLICY & PROCEDURES

Cashier Training

FOR PREPAID ACCESS PRODUCTS

POLICY EFFECTIVE DATE: 10/15/2012

Designated Policy Compliance Officers

Name: Rick Ericksen Sr. Manager, Risk Management

Phone Number: 952-915-2690

Email address: rick.ericksen@lfhi.com

Name: Rhonda Harman, Sr. Director of Human Resources

Phone Number: 952-915-2664

Email address: rhonda.harman@lfhi.com

POLICY AND PROCEDURES LIMITING SALES OF PREPAID ACCESS TO NO MORE THAN $1,000 PER PERSON PER DAY

Background

The Bank Secrecy Act (BSA), initially adopted in 1970, established the basic framework for anti-money laundering (AML) obligations imposed on financial institutions. It authorizes the Secretary of the Treasury Department (Treasury) to issue regulations requiring financial institutions and money services businesses to keep records and file reports on financial transactions that may be useful in investigations and the prosecution of money laundering and other financial crimes. The Financial Crimes Enforcement Network (FinCEN), a bureau within Treasury, is the administrator of the BSA.

Description of Money Laundering

Money laundering is the attempt to conceal or disguise the nature, location, source, ownership or control of illegally obtained money. If illegal money is successfully laundered, criminals maintain control over their illegally obtained funds and they can establish a separate cover for their illicit source of income.

Money laundering is not limited to cash. Money laundering can be done through any type of financial transaction, including, but not limited to, funds transfers, money orders, checks, debit cards, Prepaid Access such as stored value cards, and credit card transactions.

FinCEN Requirements for Sale of Prepaid Access

On July 26, 2011, FinCEN issued a Rule (the “Rule”) amending the BSA regulations and establishing comprehensive regulatory requirements for sales of prepaid stored value cards and other prepaid access. “Prepaid Access” means stored value cards or other access devices where funds are prepaid by a customer and subsequently used to make a purchase, reload a general purpose reloadable (GPR) card, or make a phone call. Prepaid Access also includes stored value gift cards issued to customers as refunds.

Traditionally, the term "money services business" (MSB) as defined by FinCEN applies to a retailer providing certain financial services including selling or redeeming stored value, whether or not on a regular basis, for more than $10,000 per person in any single day. Relating the definition of MSB to the FinCEN Rule, a retail merchant (“retailer”) is a “Seller of Prepaid Access” if: (a) it sells Prepaid Access that is not exempt under the Rule, OR (b) it sells more than $10,000 of Prepaid Access (whether exempt or not exempt) in a single day to a single person without implementing policies and procedures reasonably designed to prevent such a sale.

Products sold by this company (including those distributed by Blackhawk Network, Inc. to our company as part of the Alliance Partner network) will be exempt under the FinCEN Rule because they will be limited to no more than $1000.00 per day for (a) closed loop stored value products (i.e., loaded and reloaded onto) and will not permit cash redemptions (except as legally required); and (b) open loop stored value products prior to obtaining customer identification. Do not permit (i) international usage; (ii) person-to-person transfers or (iii) reloads from non-depository sources.

Our company is implementing this policy to avoid the sale of more than $1,000 of Prepaid Access in a single day to a single person, and to avoid being a “Seller of Prepaid Access” as a result of violating the prohibitions on such sales without this policy and procedures being in place.

Statement of Policy

We sell Prepaid Access products. “Prepaid Access” means stored value cards or other access devices where funds are prepaid by a customer and subsequently used to make a purchase, reload a general purpose reloadable (GPR) card, or make a phone call. Prepaid Access also includes stored value gift cards issued to customers as refunds.

This company supports the fight against money laundering and terrorism and has adopted this anti-money laundering policy (“Policy”) to prevent its financial services from being used to promote or execute such activity, as follows:

(1) It is our policy NOT to sell Prepaid Access under a prepaid program that can be used before the user’s identification needs to be verified except as permitted under the FinCEN Rule.

(2) It is our policy NOT to sell Prepaid Access products in excess of $1,000 to any person in a single day.

  (a) The restrictions on the sale of Prepaid Access are not limited to cash tenders, but apply to all tenders of payment.

  (b) The sale of Prepaid Access to other businesses for further distribution or sale to end users/consumers by those other businesses is not subject to the FinCEN Rule and may exceed $10,000 in one day. Any such business-to-business transactions will be completed by LFHI Accounting office.

  (c) The company will determine whether there are viable efficient technologies available to restrict purchases of Prepaid Access to less than $1,000 at the point of sale. If practical, such technologies will be used to prevent the sale, loading or reloading of Prepaid Access in excess of $1,000 to any person in a single day.

(3) Regarding customer transactions, it is our policy:

  (a) NOT to accept or disburse more than $1,000 in cash in any one day to/from any person or on behalf of another person for any transaction, including the purchase of Prepaid Access.

  (b) NOT to permit sales of Prepaid Access through self service checkout lanes.

(4) Our employees will be trained on this Policy and related procedures as part of new employee orientation and at least annually thereafter. Employees must acknowledge participation in training and an understanding of training content. Signed acknowledgement forms will be retained in employee training files.

Transaction Limits for Prepaid Access

In order to prevent sales of Prepaid Access in excess of $1,000 to any one person in a single day, employees must follow these procedures and transaction limits. Employees must understand these procedures and must direct customers to a manager when it is not clear whether a transaction should proceed.

- Employees will not allow any person to purchase or reload more than **$1,000** of Prepaid Access products (e.g., closed loop gift cards, open loop gift cards, mobile top-up cards, e-wallets, etc) in a single day.

Unusual or Suspicious Activity

Many factors are involved in determining whether transactions are suspicious, including, but not limited to the amount, the location of the store, or comments made by the customer.

"Structuring" is the act of breaking up a large transaction into several smaller transactions to avoid providing personally identifying information for store records. Many money launderers are familiar with the dollar thresholds that require record keeping and reporting. To remain anonymous and avoid detection by law enforcement officials, money launderers attempt to process transactions to avoid triggering record keeping and/or reporting requirements.

Employees must be trained to pay attention to customers who appear to be using structuring or other methods to exceed the limits in this policy or to avoid providing identification.

Employees will report all suspicious activity to the store management or designated Policy compliance officer regardless of the dollar amount. Examples of suspicious behaviors are:

- A group of customers who come in together and seem to purchase or reload Prepaid Access separately in order to avoid the threshold for the amount of Prepaid Access or number of Prepaid Access devices or vehicles that can be purchased or reloaded.
- A customer who typically buys small ticket items has an unusually large amount of cash and is purchasing multiple gift cards for no apparent legitimate reason.
- A customer uses two or more locations or cashiers in the same day in order to break one transaction into smaller ones.
- A customer wants to void the transaction once his/her identification is requested or required.
- A customer is unable or unwilling to provide valid identification.
- A customer who makes any statements that suggest that funds may be related to criminal activity.

If an employee observes a customer attempting to purchase Prepaid Access devices in excess of $1,000 during the same day, whether in one or more transactions or involving the purchase of one prepaid card or several prepaid cards, the employee must decline the sale.

(1) If an employee has actual knowledge of a prior Prepaid Access purchase by a customer who wants to purchase additional Prepaid Access cumulatively totaling more than $1,000 during the same day, the employee should advise the customer of this company's Policy in accordance with (3) below.

(2) When addressing a customer who desires to purchase more than $1,000 of Prepaid Access in one day, the employee should remain polite and professional. Simply inform the customer that it is store policy not to sell Prepaid Access with loads or reloads that total in excess of $1,000 in a single day to the same customer.

(3) If the manager determines that the activities are indeed suspicious for the reasons cited above or for any other reason, no Prepaid Access should be sold to the individual or individuals involved in the activity at that time or on any future occasion.

(4) If an individual or individuals engaging in suspicious activities persist in attempting to purchase Prepaid Access, the employee must notify the store management who will determine if it is necessary to contact loss prevention and local law enforcement for assistance.

Reporting Requirements for Suspicious Activity

Store management will follow reporting requirements as outlined in the Anti Money Laundering Policy. As an agent of Blackhawk Network, Inc., our company will provide the information necessary for Blackhawk Network, Inc. to investigate suspicious activities related to its products in accordance with the following:

Employee Education and Training

The store management or designated Policy compliance officer is responsible for ensuring that all new and existing store employees involved in the sale of Prepaid Access or Stored Value cards are familiar with this Policy and related procedures, and thresholds.

(1) Employees involved in the selling of Prepaid Access or Store Value cards should be aware of:

  (a) Specific transaction limits (as described above);

  (b) Procedures for obtaining manager approval for certain transactions (as described above);

  (c) Signs of unusual or suspicious activity (as described above); and

  (d) Procedures for reporting unusual or suspicious activity as described above.

(2) Employees must acknowledge participation in training and store management or designated Policy compliance officer must maintain a record of employees' acknowledgement of the training received.

Contact for Information

Employees should contact the store management or designated Policy compliance officer with any questions about the Policy and these procedures.