ANTI-MONEY LAUNDERING POLICY & PROCEDURES

FOR PREPAID ACCESS PRODUCTS

POLICY EFFECTIVE DATE:

Designated Policy Compliance Officer

Name: _____

Title: _____

Phone Number: _____

Email address: _____

POLICY AND PROCEDURES LIMITING SALES OF PREPAID ACCESS TO NO MORE THAN $10,000 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. Among other things, 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. The AML laws apply to any funds derived from illegal activities, such as funds held by human smugglers, drug traffickers, terrorists, organized crime, tax evaders and other groups and individuals seeking to transfer, spend and/or invest money derived from any type of crime.

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 $1,000 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: (a) closed loop stored value products that permit no more than $2,000 to be associated with (i.e., loaded and reloaded onto) the product per day and that do not permit cash redemptions (except as legally required); and (b) open loop stored value products that permit no more than $1,000 to be associated with the product per day and that, 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 $10,000 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.

TABLE OF CONTENTS

In the following statement of policy and related procedures, this company is referred to as "we," "us," or "our."

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 $10,000 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 (including, for example, credit cards) that total more than $10,000.

   (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 that exceed $10,000 will be completed only after the information that identifies the business making the purchase has been collected.

   (c) Marketing material or other advertising by our company about Prepaid Access will not indicate or suggest to customers that the Prepaid Access sold by our company can be purchased, loaded or reloaded for more than $10,000 in a day.

   (d) The company will determine whether there are viable efficient technologies available to restrict purchases of Prepaid Access to less than $10,000 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 $10,000 to any person in a single day.

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

   (a) NOT to accept or disburse more than $10,000 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.

   (c) NOT to accept credit cards for the sale of general purpose reloadable cards.

(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 personnel files and/or with employee training files.

(5) The company will periodically conduct an independent review of this Policy to determine its effectiveness and make changes where deemed prudent to mitigate money laundering risks. This review may be conducted by an outside entity or an internal department, such as the internal audit department, that is not involved with day to day sales of Prepaid Access.

(6) The Board of Directors (or its designee) and/or senior management shall approve this Policy and any updates thereto, designate a Policy compliance officer, and be responsible for the overall implementation of this Policy.

(7) This Policy applies to all store locations managed by this company. A copy of this Policy, as updated from time to time, will be made available at each location and accessible to all employees involved with the sale of Prepaid Access.

(8) The Policy and procedures do not replace but are intended to work in conjunction with our existing loss prevention program, shrink awareness program or other program for preventing theft, along with our existing training of store-level personnel in connection with that program.

(9) All questions related to this Policy must be addressed to the designated Policy compliance officer or to the store manager on duty.

Policy Oversight

The designated Policy compliance officer is responsible for:

- Liaising with Blackhawk Network on all matters involving possible money laundering resulting from the sale of Blackhawk Network's distributed products.
- Monitoring changes in our business to ensuring ongoing compliance with federal and state specific AML regulations.
- Implementing and ensuring day-to-day compliance with corporate policies and procedures contained in this Policy.
- Overseeing or managing the reporting process to ensure that all reports and all records are maintained in compliance with federal, state and Blackhawk Network, Inc. requirements.
- Cooperating with law enforcement and Blackhawk Network, Inc. on investigations
- Developing and implementing a training program to ensure that all employees receive appropriate training with regard to this Policy, and documenting employee participation in such training.
- Serving as the designated person to whom suspicious activity at retail locations is referred for further action.
- Ensuring that periodic reviews of this Policy are conducted.

Procedures Limiting Sales of Prepaid Access to no more than $10,000 per Person per Day

I. Transaction Limits for Prepaid Access

In order to prevent sales of Prepaid Access in excess of $10,000 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.

(1) 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.

(2) **Total Prepaid Access sales exceeding $1,000 but no more than $10,000:** With manager approval, employees may allow the purchase of Prepaid Access totaling more than $1,000 but no more than $10,000. For such purchases, the sales employee must obtain and record customer identifying information including but not limited to:

- (a) Transaction date and time
- (b) Customer name
- (c) Customer address
- (d) Customer's valid, unexpired government issued photo ID. Acceptable forms are:
  - (i) Driver's License (state or territory)
  - (ii) State ID
  - (iii) Provisional Driver's License
  - (iv) Passport
  - (v) US Military Card
  - (vi) Native American Tribal ID
  - (vii) Welfare ID
  - (viii) Inmate (Exit Prison) ID
  - (ix) Resident Alien Card
  - (x) Temporary Resident Card (US Dept. of Justice)
  - (xi) Employment Authorization Card (US Dept. of Justice
- (e) Number and denomination of Prepaid Access purchased
- (f) Payment type [cash, check, credit card, debit card].
  - (i) **Exception**: Credit cards must NOT be accepted for the purchase of General Purpose Reloadable (GPR) cards
- (g) Total amount purchased
- (h) Employee number of employee who conducted the transaction
- (i) Name of employee who conducted the transaction
- (j) Manager's approval

(3) The store manager or designated Policy compliance officer should maintain a record of all such approvals and transactions. Sample log for recording purchases exceeding $1000 is included in this document under ***Appendix 1*** to this Policy.

(4) If there is any doubt whether an additional purchase or reload would exceed the maximum allowable $10,000 per person per day threshold, including if, for example, store personnel see a customer make multiple purchases in a day, store personnel must not permit the additional purchase or reload.

(5) **"Bulk" sales of Prepaid Access to businesses:** If a customer represents a business and would like to make a Prepaid Access purchase on behalf of that business for a total value of more than $10,000, the sales employee must obtain and record customer identifying information including but not limited to:

(a) Transaction date and time
(b) Business Name
(c) Principal place of business address (not P. O. Box)
(d) Business telephone number (including area code)
(e) Business Federal Tax ID (EIN/TIN)
(f) Business contact name
(g) Business contact's valid, unexpired government issued photo ID. Acceptable forms are:
    (i) Driver's License (state or territory)
    (ii) State ID
    (iii) Provisional Driver's License
    (iv) Passport
    (v) US Military Card
    (vi) Native American Tribal ID
    (vii) Welfare ID
    (viii) Inmate (Exit Prison) ID
    (ix) Resident Alien Card
    (x) Temporary Resident Card (US Dept. of Justice)
    (xi) Employment Authorization Card (US Dept. of Justice
(h) Number and denomination of Prepaid Access purchased
(i) Payment type [cash, check, credit card, debit card]. **Exceptions:**
    (i) **Exception**: Cash must NOT be accepted for purchase amount greater than $10,000
    (ii) **Exception**: Credit cards must NOT be accepted for the purchase of General Purpose Reloadable (GPR) cards
(j) Total amount purchased
(k) Description of how cards will be used (e.g., corporate gifting, resale for profit, resale not for profit)
(l) Employee number of employee who conducted the transaction
(m) Name of employee who conducted the transaction
(n) Manager's approval

(6) The store manager should maintain a record of all such approvals and transactions. Sample form for recording bulk purchases is included in this document under ***Appendix 2*** to this Policy.

II. 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, comments made by the customer, the customer's behavior and the customer's previous transaction history. It is important to understand customers and what activity is normal for each of them as there is no clear-cut definition of suspicious activity. What may be normal or suspicious for one customer may be appropriate for another.

"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 will report all suspicious activity to the store manager 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 asks a cashier how to avoid the threshold for the amount of Prepaid Access that can be purchased or reloaded.
- A customer who attempts to bribe or threaten a cashier to ignore the threshold for the amount of Prepaid Access 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 uses a false or obviously altered identification.
- A customer who makes any statements that suggest that funds may be related to criminal activity.
- The credit card that the customer wants to use to pay for the product is not working through the POS machine. The customer would like you to call into the issuing bank with the phone number that they're providing.

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.

(1) If an employee observes a customer attempting to purchase Prepaid Access devices in excess of $10,000 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 prevent the customer from doing so.

(2) 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 $10,000 during the same day, the employee should advise the customer of this company's Policy in accordance with (3) below.

(3) When addressing a customer who desires to purchase more than $10,000 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 $10,000 in a single day to the same customer.

(4) 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.

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

III. Blackhawk Network, Inc. Reporting Requirements for Suspicious Activity

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:

(1) The store manager or designated Policy compliance officer will complete a Suspicious Activity Investigation Report (IR) for suspicious transactions and notify Blackhawk Network, Inc. within two (2) calendar days from the initial date of detection of the suspicious activity. Blackhawk Network, Inc. will review the IR and submit it, along with any supporting documentation to the card issuer. Blackhawk Network, Inc. will not disclose whether or not a SAR has been filed based on our referral. A sample IR is included in the ***Appendix 3*** to this Policy.

(2) Employees must NOT alert or tell the customer involved in the suspicious transaction(s) that an IR has been or will be filed.

(3) The store manager or designated Policy compliance officer will keep copies of all records and supporting documentation from the IR referrals for a period of five years from the date of report.

IV. Procedures for Filing a Currency Transaction Report (CTR)

Federal regulations require the reporting of a cash transaction of more than $10,000 made in any one day by any person or on behalf of another person by completing a Currency Transaction Report (CTR). Multiple transactions must be treated as a single transaction if the store has knowledge that:

(1) The transactions are conducted by or on behalf of the same person, and

(2) The transactions result in either currency received (Cash In) or currency disbursed (Cash Out) totaling more than $10,000 during any one day.

However, since it is our policy NOT to accept more than $10,000 in cash in any one day from any person or on behalf of another person for any transaction, including the purchase of Prepaid Access, these reporting requirements are not applicable unless our Policy has been violated.

If a customer insists on tendering cash for a bulk purchase in excess of $10,000, the transaction must not be completed and as much information as possible must be collected to file an IR.

V. Employee Education and Training

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

(1) Employees involved in the selling of Prepaid Access 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) The Policy and related procedures will be provided and explained to applicable existing employees, as necessary, and to all applicable new employees upon hire and at least annually thereafter.

(3) Employees must acknowledge participation in training and the store manager or designated Policy compliance officer must maintain a record of employees' acknowledgement of the training received as set forth in ***Appendix 4*** to this Policy.

VI. Additional Requirements for Store Locations in the State of Arizona

The State of Arizona requires the following additional information:

(1) Additional **data retention** requirements: For each transaction originating in the State of Arizona, the following information will be retained:

   (a) The name of the partner, merchant, agent, and the street address of the location where the money was received;

   (b) The name and street address of the customer if reported to the licensee or authorized delegate;

   (c) The approximate date of the transaction;

   (d) The name or other information required to determine the identity of the employee of the partner, merchant or agent who conducted the transaction; and

   (e) The amount of the transaction.

(2) Additional **training** requirements:

   (a) All employees will be trained regarding the relevant statutes and the criminal penalties for failure to comply with all reporting, monitoring and data retention requirements.

   (b) Training will also include details of criminal penalties and consequences for falsification of documentation.

VII. Monitoring and Remediation

Transactions will be monitored periodically to ensure compliance with this Policy by all employees. Our company will also perform testing to ensure that all channels of distribution are fully compliant with the FinCEN Rule.

(1) If more than $10,000 was sold to one person on the same day, determine the reason why the Policy violation occurred and initiate appropriate remediation to prevent its recurrence.

(2) Discipline each employee who does not comply with the Policy and procedures (including suspension or termination).

(3) Conduct periodic independent reviews of compliance with the Policy and procedures and take any necessary corrective actions.

(4) Review the Policy and procedures for effectiveness and update as necessary.

VIII. Law Enforcement Requests

Law enforcement agencies or regulators may request information and records. Employees must direct all such requests to the store manager. The store manager must cooperate with requests from these agencies: however, the store manager must not release consumer or company information without first receiving proper summons, subpoena or court order. This is necessary to ensure that we comply with customer privacy laws.

IX. Contact for Information

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

X. Additional Resources

(1) The FinCEN final rule publication (July 16, 2011):
http://www.fincen.gov/news_room/nr/pdf/20110726b.pdf

(2) Frequently asked questions related to the FinCEN final rule:
http://www.fincen.gov/news_room/nr/pdf/20111102.pdf

APPENDIX 1: Log for Prepaid Access Sales Exceeding $1,000 but less Than $10,000

(Cut along perforated line, copy and distribute for internal use)

Log for Prepaid Access Sales Exceeding $1,000 but Less Than $10,000

For Prepaid Access sales exceeding $1,000 but no more than $10,000 to a single person in a single day, the following log must be completed.

Note: Customer's ID must be valid, unexpired government issued photo ID. Acceptable Customer ID Types are:

- Driver's License (state or territory)
- State ID (state or territory)
- Inmate (Exit Prison) ID
- Resident Alien Card
- Provisional Driver's License (state or territory)
- Temporary Resident Card (US Dept. of Justice)
- Employment Authorization Card (US Dept. of Justice
- Native American Tribal ID
- Welfare ID
- Passport (country)
- US Military Card

	(a) Transaction Date	(b) Customer Name	(c) Customer Address	(d) Customer ID Type & Number/Ref	(e) Number and Denomination of Prepaid Access Purchased			(g) Payment Type	(h) Employee Name	(i) Employee Number	(j) Manager Signature
1					Card Value	Number Purchased	Total ($)	☐ Cash ☐ Check ☐ Credit Card ☐ Debit Card			
						(f) Total Amount					
2					Card Value	Number Purchased	Total ($)	☐ Cash ☐ Check ☐ Credit Card ☐ Debit Card			
						(f) Total Amount					
3					Card Value	Number Purchased	Total ($)	☐ Cash ☐ Check ☐ Credit Card ☐ Debit Card			
						(f) Total Amount					

APPENDIX 2: Form for Business Purchase of Prepaid Access Over $10,000

(Cut along perforated line, copy and distribute for internal use) -

Form for Business Purchase of Prepaid Access in Excess of $10,000

Complete this form for a Prepaid Access amount totaling more than $10,000 sold to an individual or group making the purchase on behalf of a business for further distribution or resale. Retain this form for your records.

Transaction Date	
Reason for purchase *(e.g. corporate gifting, resale for profit, resale not for profit etc.)*	
Business Name *(Business legal entity, or business operating name)*	
Business Address *(Physical address of business, no P.O. Box)*	
Business Federal Tax ID (EIN/TIN)	
Business Contact Name *(First and Last Name of individual providing payment on behalf of business)*	
Contact Identification *(Select one and enter identification number)*	□ Driver's License □ State ID □ Passport □ US Military Card □ Resident/Temp Alien Card □ Other (write)_____ **Selected ID Number:**_____

Card Description	Card Face Value ($)	Number of Cards Purchased	Total ($)
		Total Transaction Amount ($)	

Employee/Associate Name	
Employee Number	
Manager Name	
Manager Signature	

APPENDIX 3: Suspicious Activity Investigation Report

(Cut along perforated line, copy and distribute for internal use) -

Suspicious Activity Investigation Report (IR)

Blackhawk Network will use this report to investigate reported unusual or suspicious activity. Please complete in its entirety and be specific. If not all details are known, complete as many as feasible. Attach copies of all supporting documentation and send via email to investigations@bhnetwork.com to the attention of the Blackhawk Risk Analyst Maintain original supporting documentation in a secure location. **All emails must be sent via secure, encrypted email.**

Agent Information	
Company name:	
Company address:	
Suspicious Activity Investigation Report completed by:	
Contact phone number:	
Contact email	
Report Details	
Date of report:	
Has law enforcement been notified?	
If yes, what agency?	
Name of person contacted:	
Phone number of contact:	
Subject Information (Person or persons whose activities are deemed to be suspicious)	
Subject name and/or relationship: (customer, employee, owner, etc.)	
Subject's street address:	
Subject account number:	
If an employee, are they still employed?	
If no, resignation, termination, or suspension?	
Date of termination/resignation:	
Subject's home phone number:	
Subject's work phone number:	
Subject's Tax ID Number:	
Subject's birth date:	
Subject's occupation:	
Has subject admitted or confessed to illegal activity?	

APPENDIX 3: Suspicious Activity Investigation Report

(Cut along perforated line, copy and distribute for internal use) -

Suspicious Activity Information	
Date or date range of suspicious activity:	
Date unusual activity first detected:	
Date investigation completed:	
Total dollar amount involved:	
Number and Denomination of cards purchased:	
Payment type:	
Amount of loss prior to recovery:	
Dollar amount of recovery:	
Summary of suspicious activity (mark all that apply):	___ Structuring/Money Laundering ___ Bribery ___ Check Fraud ___ Counterfeit Credit/Debit Card ___ Debit Card Fraud ___ Credit Card Fraud ___ Counterfeit Instrument ___ Prepaid Card Fraud ___ Embezzlement ___ False Statement ___ Misuse of Position ___ Mysterious Disappearance ___ Wire Transfer Fraud ___ Terrorist Financing ___ Identity Theft ___ Other (specify) _____

Detailed Narrative:

APPENDIX 4: Sample Employee Training Sign-Off Sheet

(Cut along perforated line, copy and distribute for internal use) -

Employee Training Sign-Off Sheet

I have been trained and understand this Anti-Money Laundering Policy and Procedures.

Row #	Print Name	Signature	Date
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

Store #: _____

Store Address: _____

Manager Name: _____

Manager Signature: _____