

EXPRESS MORTGAGE GROUP, INC. IDENTIFY THEFT PREVENTION PROGRAM

Scope

The following pages contain the Identity Theft Prevention Program ("Red Flags Program") for our company. It contains the policies and procedures adopted by our company pursuant to the FTC's Red Flags Rule (16 CFR § 681.2(d)).

Definitions

1. Company Name: **EXPRESS MORTGAGE GROUP, INC.**
2. Approving Officer or Board of Directors: **Donna M. Staley**
3. Covered Accounts: **Mortgage Loans**
4. Staff: employees who are involved collecting or have access to information relating to the Mortgage Loan
5. Service Providers: Service Providers include any person or organization providing services to the Company that may have access to the information contained in Accounts

Creating and Maintaining the Program

Responsibilities: Our company elects to have a Red Flags Manager. The Red Flags Manager is responsible for:

- Conducting an initial and periodic risk assessment to identify the accounts that could be susceptible to identity theft risks.
- Creating and updating this Red Flags Program, which includes identifying relevant Red Flags, implementing methods to detect them, and creating processes to respond appropriately when they are detected.
- Training of appropriate Staff
- Reporting important issues relevant to the Program to appropriate Board of Directors or Officers of the Company

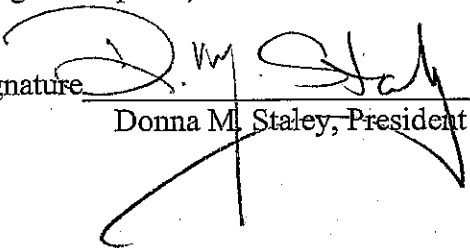
Designation of Red Flags Manager

I, **Donna M. Staley**, do hereby accept the position of Red Flags Manager for my employing company. I understand my duties will include, but will not be limited to, the following:

1. Familiarizing myself with the FTC's Red Flags Rule and related requirements
2. Overseeing, developing, implementing, and administering our written Red Flags Program
3. Having our Red Flags Program approved by the Board of Directors (or other personnel as this Program requires)
4. Assessing risks of identity theft with respect to "covered accounts"
5. Training employees on our Red Flags Program
6. Making myself reasonably available so that employees or service providers may ask questions, report concerns, and/or seek approval for waivers with respect to our Red Flags Program
7. Overseeing the contracting with service providers pursuant to this Red Flags Program
8. Communicating regularly with the finance companies with which we work to ensure this Red Flags Program is consistent with their requirements
9. Maintaining copies of Red Flags-related policies and documents issued by the finance companies with which we work
10. Updating this Red Flags Program as necessary
11. Discussing possible disciplinary measures with senior management if an employee is found to have either negligently or intentionally violated the requirements of this Red Flags Program
12. Periodically reporting important issues relevant to the Red Flags Program to the Board of Directors (or other personnel as this Program requires)

Date 5.1.09

Employee Signature


Donna M. Staley, President

Risk Assessment

1. As part of this Program development, we must conduct a risk assessment to determine whether we offer or maintain "covered accounts" taking into consideration the following "Risk Factors":
 - The methods we provide to open our "accounts";
 - The methods we provide to access our accounts; and
 - Our previous experiences with identity theft.
2. This Program will include existing Red Flags that the Program Manager has determined are an effective means of detecting identity theft. (see Exhibit 1 – Response Matrix)

Updating and Reporting on the Program

1. **Updates:** The Program Manager will update this Program and take into consideration the following:
 - The Company's experiences with identity theft
 - Recognized changes in methods of identity theft (from associations and industry sources)
 - Changes in methods to detect, prevent and mitigate identity theft
 - Changes in the types of Accounts the Company offers or maintains and
 - Changes in the Company's business arrangements
2. **Reporting:** At least annually, or in the event of any significant incidence of identity theft, the Program Manager will prepare a report reviewing the effectiveness of this Program and recommend any changes to the Program.
 - a. The report should address any significant matters related to identity theft detection and mitigation and evaluate:
 - The effectiveness of the Program with respect to its effectiveness at detecting and mitigating identity theft in the course of opening Accounts;
 - Service provider arrangements;
 - Any Significant incidents involving identity theft and management's response; and
 - Changes that should be incorporated into the Program.
 - b. All updates to this Program will be documented and appended to this Program as a written appendix, log, or notation.

Identifying Red Flags

1. **Identifying Red Flags:** Red Flags associated with the origination or maintenance of the Company's Accounts are identified by the Program Manager as she considers:
 - a. The methods used to open Accounts (in person, via phone, internet submission, etc.) This includes our Customer Identification methods.

- b. The methods and procedures that the Company employs to allow access to Account information
- c. The Company's previous experiences with identity theft

 X We have NO experience with identity theft

2. **Sources of Red Flags:** The Program Manager will identify Red Flags to be part of this Program from the following sources:
 - a. The Company's current policies and procedures
 - b. The Company's experience with prior identity theft
 - c. New methods of identity theft that we have identified that reflect changes in identity theft risks
 - d. Applicable supervisory guidance
3. **Categories and Specific Red Flags:** These Categories of Red Flags and specific Red Flags are labeled in the **Exhibit 1 – Response Matrix**, and updated per guidelines above.

Detecting Red Flags

Detecting and evaluating Red Flags at application

Perhaps the most essential element of our Red Flags program is the detection of those Red Flags previously identified. We detect Red Flags as follows:

1. **Credit Application information:** containing at least:
 - a. Full Name of all Applicants
 - b. Date(s) of birth
 - c. Address, Army Post Office, Fleet Post Office, or principal place of business or other physical location.
 - d. Identification number (social security number with state of issuance), or:
 - a taxpayer identification number (TIN),
 - 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 similar safeguard
2. **Personal Behavior Red Flags:** These Red Flags have been identified as patterns of personal behavior that can warrant further documentation and investigation, as we deem necessary, using the facts and circumstances surrounding the incident.
 - Customer appears unusually nervous and/or agitated
 - Customer is pressuring Company personnel to rush through the origination process
 - Customer appears unusually disinterested in the terms of the loan
 - Customer conducts all negotiations via telephone/email/internet and does not intend to present ID and/or sign paperwork

3. **Verifying Identification:** The Company elects to use a Customer Identification Checklist (Exhibit 2). The Checklist will be maintained with the applicant's credit file. The Program Manager will update the Checklist from time to time as needed to comply with the objectives of the Program.

a. **Acceptable Documentation:** Acceptable documentation for identity verification purposes includes: ****(MUST BE PRESENTED AT INITIAL APPLICATION)****

- Current Driver's License -
- Current Passport
- Government-issued Identification Card, containing photograph or similar safeguard,
- Articles of Incorporation
- Government-issued Business License

Questions about the authenticity of the identification should be referred to the Program Manager.

b. **Additional Authentication:** In the event the Company originates a loan without being the physical presence of the customer (i.e. a phone or internet application), additional steps need to be taken to authenticate their identities:

- i. Contact the customer by telephone on multiple occasions, via multiple means (more than one phone number at different times)
- ii. Use a third-party identity verification tool which provides a "pass/fail" response.
- iii. Ask the customer questions and determine if the responses match information delivered from the consumer report or other third-party sources, such as:
 - The amount of their current mortgage payment
 - The balance on a current auto loan
 - Approximate balances on current credit cards
 - Names of current creditors
 - Prior addresses where the customer lived
 - Names of employers
- iv. Check references with other parties (employers, creditors, etc.).
- v. Obtain additional documentation from the customer or other sources

c. **Verifying customer-provided information**

- i. Validate the customer's SSN using third-party verification tools or other means.
- ii. Use tools such as www.socialsecurity.gov/employer/stateweb.htm to determine if the Social Security Number provided matches states and dates of issue.
- iii. If a consumer report has a notice of address discrepancy, ask the customer about the reason for the discrepancy and ask for additional documentation to verify the address (a utility bill, phone record, insurance statement, etc.).
- iv. Use third-party services to determine whether the address provided by the customer is associated with fraud or identity theft.

If information cannot be reconciled or validated, escalate to the Program Manager for action.

d. **Credit Reporting Alerts, Suspicious Activity, and Credit Freezes**

1. **Active duty alerts:** If the customer's consumer report contains an active duty alert, obtain a military ID from the customer, as well as orders indicating where consumer is stationed. If the customer is unable to provide documentation, escalate to the Program Manager for action.
2. **Initial and Extended Fraud alerts:** If the consumer report indicates the presence of any type of fraud alert, additional photo identification will be required. The contact information provide in the alert will be used, and any and all additional efforts to verify the identity of the consumer will be documented.
3. **Suspicious Account Activity:** Review all consumer reporting data carefully for suspicious activity. If any suspicious activity is present, ask the customer about the reasons for the activity. If the customer cannot explain or behaves suspiciously, escalate to the Program Manager for action. Suspicious activity includes:
 - A recent increase in the volume of inquiries
 - An unusual number of new accounts
 - A significant change or substantial use of credit, especially with respect to new accounts (significant balances on credit cards that have otherwise been relatively inactive or only moderately active)
 - An account that was closed for abuse by a financial institution or creditor
4. **Credit freezes:** In the event that a credit report is denied due to a credit freeze, advise the customer that he or she will have to provide his or her personal identification number (PIN) to the consumer reporting agency unfreeze the file. If the customer does not remember the PIN, direct him or her to the consumer reporting agency for assistance. If the customer does not recall his or her PIN and is unable to thaw the file after working with the consumer reporting agency, escalate to the Program Manager for action
5. **Customer/Law Enforcement notices:** The Company maintains a file of notices from customers, law enforcement, victims of identity theft and others who have advised of identity theft activity relating to certain names, addresses, phone numbers and SSNs. All Account applications should be checked against such file prior to approval.

e. **Office Security Procedures:** The Company maintains a secure office.

- i. No files are left out on desk unless they are in use.
- ii. All files are encrypted.
- iii. No documents are printed from home.
- iv. No files are taken home.

- f. **Existing Accounts:** As a mortgage broker, accounts are not typically serviced by the Company. In the event that an Account must be temporarily serviced, we will take the following additional actions:
- i. In the event of a first payment default, efforts will be made to contact the customer to determine the cause for the default.
 - ii. In the event of a payment default when there is no history of late or missed payments, efforts will be made to contact the customer to determine the cause for the default.

If the customer cannot be contacted and it is believed that a fraud or identity theft has occurred, the Program Manager will contact law enforcement or take such other action as may be necessary and proper to protect the Company and its customers.

- iii. All new Accounts and all existing Accounts will be monitored for known fraud patterns.

Preventing and Mitigating Identity Theft ("Responding to Red Flags")

1. General

- a. When a Red Flag is detected, the Staff will follow the appropriate responses detailed in **Exhibit 2** or in a manner otherwise consistent with the objectives of this Program, as deemed appropriate for facts and circumstances of the Red Flag. All actions will be documented.
 - b. If a Red Flag cannot be resolved with reasonable certainty, it will be escalated to the Program Manager for determination on best course of action.
 - c. All Red Flags should be resolved prior to opening an Account. A transaction where there is an unresolved Red Flag cannot proceed unless it is documented and authorized by the Program Manager.
2. **Responses.** Accepted responses to Red Flags are described below (and as noted and updated in Exhibit 1). Appropriate responses are determined as we perceive the level of risk using the facts and circumstances of the nature of the Red Flag:
- Determining that no response is necessary
 - Requiring satisfactory explanation from the customer
 - Requiring additional documentation from the customer, e.g., additional satisfactory photo identification
 - Obtaining more identifying information from the customer, e.g., a utility bill showing the customer's name and address or the use of third-party fraud detection and/or identity verification tools
 - If the customer's identify can not be authenticated, not opening the Account
 - Escalating the Red Flag to the Program Manager for action
 - Notifying Law Enforcement
 - For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation

Updating the Program

No less often than once per year, we update this Program. These updates include a review of the current Red Flags and a determination must be made whether additional Red Flags must be added to the Program. The updates must reflect changes in risks to customers or to the financial safety of the Company with respect to identity theft risk.

The following are triggering events which may require an update of this Program:

- Any experiences with identity theft
- Changes in how identity theft is occurring generally
- Changes in the ways identity theft is detected, prevented, and mitigated
- Changes in the types of accounts that we offer or maintain
- Changes in the types of transactions we conduct or the way we conduct them
- Changes in our business arrangements, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Anytime an update occurs, a risk assessment must be conducted per Section C.5 of this Program.

All Program updates must be must be logged and appended to this Program.

Exhibit 1 – Response Matrix

Category of Red Flag	Red Flag	Detection	Possible Response
<p>Alerts, notifications, or other warnings received from</p> <p><input type="checkbox"/> Consumer Credit Reporting Agencies, or</p> <p><input type="checkbox"/> Service providers, such as fraud detection services;</p>	<p>A fraud or active duty alert is included with a consumer report.</p>	<p><input type="checkbox"/> Check Credit Report for Fraud Alert or Active Duty Alert</p>	<p>Follow the Credit Bureau's Procedures for Consumer Credit Report Fraud Alert or Active Duty Alert</p>
	<p>A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.</p>	<p>Third-Party Red Flags Detection Solution</p>	<p>1. Third Party Red Flags Detection Passed</p> <p><input type="checkbox"/> Proceed with Transaction if other Red Flags requirements satisfied</p> <p>2. Third Party Red Flags Detection Failed</p> <p><input type="checkbox"/> Run ID Authentication Tool</p> <p>3. If Applicant fails ID Authenticate</p> <p><input type="checkbox"/> Monitor an account for evidence of identity theft;</p> <p><input type="checkbox"/> Contact the customer;</p> <p><input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account;</p> <p><input type="checkbox"/> Reopen an account with a new account number;</p> <p><input type="checkbox"/> Not open a new account;</p> <p><input type="checkbox"/> Close an existing account;</p> <p><input type="checkbox"/> Notify law enforcement</p> <p><input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;</p>
	<p>A consumer reporting agency provides a notice of address discrepancy.</p>		
	<p>A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:</p> <p><input type="checkbox"/> A recent and significant increase in the volume of inquiries;</p> <p><input type="checkbox"/> An unusual number of recently established credit relationships;</p> <p><input type="checkbox"/> A material change in the use of credit, especially with respect to recently established credit relationships; or</p> <p><input type="checkbox"/> An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.</p>		

Category of Red Flag	Red Flag	Detection	Possible Response
Presentation of Suspicious Personal Identifying Information	<p>A fraud or active duty alert is Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The address does not match any address in the consumer's data file; or <input type="checkbox"/> The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File. 	Third-Party Red Flags Detection Solution	<p>1. Third Party Red Flags Detection Passed</p> <ul style="list-style-type: none"> <input type="checkbox"/> Proceed with Transaction if other Red Flags requirements satisfied <p>2. Third Party Red Flags Detection Failed</p> <ul style="list-style-type: none"> <input type="checkbox"/> Run ID Authentication Tool <p>3. If Applicant fails ID Authenticate</p> <ul style="list-style-type: none"> <input type="checkbox"/> Monitor an account for evidence of identity theft; <input type="checkbox"/> Contact the customer; <input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account; <input type="checkbox"/> Reopen an account with a new account number; <input type="checkbox"/> Not open a new account; <input type="checkbox"/> Close an existing account; <input type="checkbox"/> Notify law enforcement <input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;
	<p>Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.</p>		
	<p>Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The address on an application is the same as the address provided on a fraudulent application; or <input type="checkbox"/> The phone number on an application is the same as the number provided on a fraudulent application. 		
	<p>Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The address on an application is fictitious, a mail drop, or a prison; or <input type="checkbox"/> The phone number is invalid, or is associated with a pager or answering service. 		
	<p>The SSN provided is the same as that submitted by other persons opening an account or other customers.</p>		
	<p>The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.</p>		

Category of Red Flag	Red Flag	Detection	Possible Response
Presentation of Suspicious Personal Identifying Information	The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.	<input type="checkbox"/> Check Application for required personal information. Is the applicant unable to provide all required personal identifying information for an application?	<input type="checkbox"/> Run ID Authentication Tool If Applicant fails ID Authentication <input type="checkbox"/> Monitor an account for evidence of identity theft; <input type="checkbox"/> Contact the customer; <input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account; <input type="checkbox"/> Reopen an account with a new account number; <input type="checkbox"/> Not open a new account; <input type="checkbox"/> Close an existing account; <input type="checkbox"/> Notify law enforcement <input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;
	Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.	<input type="checkbox"/> Check personal identifying information on application or other documents against personal identifying information currently on file. Is it consistent with personal identifying information that is currently on file?	
	For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.	<input type="checkbox"/> Applies if your Business uses Challenge (Outof-Wallet) questions – Check account if the person opening the covered account or the customer fails to answer challenge questions such as questions about places they have lived or people they know.	

Category of Red Flag	Red Flag	Detection	Possible Response
Presentation of Suspicious Documents	Documents provided for identification appear to have been altered or forged.	<input type="checkbox"/> Inspect Driver's License or other documents provided for personal identification. Does it appear to have been altered or forged upon physical inspection?	<input type="checkbox"/> Run ID Authentication Tool
	Photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.	<input type="checkbox"/> Inspect photograph and physical description on the Driver's License or other personal identification. Is it consistent with the appearance of the applicant or customer presenting the identification?	If Applicant fails ID Authentication <input type="checkbox"/> Monitor an account for evidence of identity theft;
	Other information on the identification is not consistent with information provided by the person opening a new account or customer presenting the identification.	<input type="checkbox"/> Review other information on the identification, such as the address, social security number, and date of birth. Is that information consistent with information provided by the person opening a new account or customer presenting the identification?	<input type="checkbox"/> Contact the customer;
	Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.	<input type="checkbox"/> Review other information on the identification. Is that information consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check?	<input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account;
	An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.	<input type="checkbox"/> Inspect the application presented. Does it appear to be have altered or forged, or does it give the appearance of having been destroyed and reassembled?	<input type="checkbox"/> Reopen an account with a new account number; <input type="checkbox"/> Not open a new account; <input type="checkbox"/> Close an existing account; <input type="checkbox"/> Notify law enforcement <input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;

Category of Red Flag	Red Flag	Detection	Possible Response
<p>Red Flag based on unusual use of, or suspicious activity related to, the covered account</p>	<p>Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.</p> <p>A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:</p> <ul style="list-style-type: none"> <input type="checkbox"/> The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or <input type="checkbox"/> The customer fails to make the first payment or makes an initial payment but no subsequent payments. <p>A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Nonpayment when there is no history of late or missed payments; <input type="checkbox"/> A material increase in the use of available credit; <input type="checkbox"/> A material change in purchasing or spending patterns; <input type="checkbox"/> A material change in electronic fund transfer patterns in connection with a deposit account; or <input type="checkbox"/> A material change in telephone call patterns in connection with a cellular phone account. 	<ul style="list-style-type: none"> <input type="checkbox"/> Check when receiving a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account. Has there been a recent notice of a change of address? <input type="checkbox"/> Applies to Revolving Credit Accounts - Inspect revolving accounts to detect when a majority of available credit on a revolving account is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry). <input type="checkbox"/> Applies to Revolving Credit Accounts - Inspect revolving accounts to detect when the customer fails to make the first payment or makes an initial payment but no subsequent payments. <input type="checkbox"/> Check covered accounts that are delinquent when there is no history of late or missed payments. <input type="checkbox"/> Applies to Revolving Credit Accounts, Checking Accounts etc. Check covered accounts where there is a material increase in the use of available credit on a covered account. <input type="checkbox"/> Applies to Revolving Credit Accounts, Checking Accounts etc. - Check covered accounts where there is a material change in purchasing or spending patterns by a customer on a covered account. <input type="checkbox"/> Applies to Deposit and Checking Accounts - Check covered accounts where there is a material change in electronic fund transfer patterns in connection with a deposit account. <input type="checkbox"/> Applies to Cellular Phone Accounts - Check covered accounts where there is a material change in telephone call patterns in connection with a cellular phone account. 	<ul style="list-style-type: none"> <input type="checkbox"/> Run ID Authentication Tool If Applicant fails ID Authentication <input type="checkbox"/> Monitor an account for evidence of identity theft; <input type="checkbox"/> Contact the customer; <input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account; <input type="checkbox"/> Reopen an account with a new account number; <input type="checkbox"/> Not open a new account; <input type="checkbox"/> Close an existing account; <input type="checkbox"/> Notify law enforcement <input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;

Category of Red Flag	Red Flag	Detection	Possible Response
<p>The Unusual Use of, or Suspicious Activity related to, a Covered Account</p>	<p>A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).</p>	<p><input type="checkbox"/> Applies to Revolving Credit Accounts, Checking Accounts etc.</p> <p>Inspect usage of a covered account (such as a revolving account) that has been inactive for a reasonably lengthy period of time (taking into account the expected pattern of usage and other relevant factors).</p>	<p><input type="checkbox"/> Run ID Authentication Tool</p> <p>If Applicant fails ID Authentication</p>
	<p>Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.</p>	<p><input type="checkbox"/> Check covered accounts where mail that has been sent to the customer is returned repeatedly as undeliverable. Have transactions continued to be conducted in connection with the customer's covered account.</p>	<p><input type="checkbox"/> Monitor an account for evidence of identity theft;</p> <p><input type="checkbox"/> Contact the customer;</p>
	<p>The financial institution or creditor is notified that the customer is not receiving paper account statements.</p>	<p><input type="checkbox"/> Check a covered account upon receiving notice by the customer that the customer is not receiving paper account statements.</p>	<p><input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account;</p> <p><input type="checkbox"/> Reopen an account with a new account number;</p>
	<p>The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.</p>	<p><input type="checkbox"/> Check a covered account upon receiving notice of unauthorized charges or transactions in connection with a customer's covered account.</p>	<p><input type="checkbox"/> Not open a new account;</p> <p><input type="checkbox"/> Close an existing account;</p> <p><input type="checkbox"/> Notify law enforcement</p> <p><input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;</p>

Category of Red Flag	Red Flag	Detection	Possible Response
Receipt of Notice from: <input type="checkbox"/> Customers, <input type="checkbox"/> Victims of Identity Theft <input type="checkbox"/> Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with "Covered Accounts" held by your Financial Institution or Business	Your business has been notified by: <input type="checkbox"/> a Customer <input type="checkbox"/> a Victim of Identity Theft <input type="checkbox"/> a Law Enforcement Authority, or <input type="checkbox"/> any other person that Your Business has opened a fraudulent account for a person engaged in identity theft.	Receipt of Notice	<input type="checkbox"/> Monitor an account for evidence of identity theft; <input type="checkbox"/> Contact the customer; <input type="checkbox"/> Change any passwords, security codes, or other security devices that permit access to a customer's account; <input type="checkbox"/> Reopen an account with a new account number; <input type="checkbox"/> Not open a new account; <input type="checkbox"/> Close an existing account; <input type="checkbox"/> Notify law enforcement <input type="checkbox"/> For those that are subject to Bank Secrecy Act (31 U.S.C. 5318(g)), filing a Suspicious Activity Report in accordance with applicable law and regulation;

Exhibit 2

Customer Identification Checklist

1. **This applicant is:** An Individual Business

2. Customer Contact Information

Name: _____

Address: _____

City / State / Zip _____

SSN/TIN obtained? (maintained in file): Yes No

DOB (Individual Customer Only) _____

If a Business, please indicate type:

Corporation Partnership Trust Sole Proprietorship Other

3. Documentation Obtained:

Individual

- Driver's License
State: _____
Expiration Date: _____
Number: _____
- U.S. Passport
Date of Issue: _____
Expiration Date: _____
Number: _____
- Other
Date of Issue: _____
Expiration Date: _____
Number: _____
Describe: _____

Business

- Photo ID provided? Yes No
- Articles of Incorporation
- Business License
- Partnership Agreement
- Other (describe): _____

4. Automated Fraud Detection Services

Clear (none present or no match)

Other _____

5. Verification

I have examined the document(s) presented by the above-named customer and that the above-listed document(s) appear to genuine and related to the named customer. [If the employee completing this form cannot make this certification, the Red Flags Manager must approve the transaction. If the employee completing this form can make this certification, the Red Flags Manager’s approval is not required]

Name: _____

Signature: _____

Date: _____

5. Was this Customer Identification Checklist reviewed by the Red Flags Manager?

Yes No

If you answered “Yes,” please complete the following information:

Name of Red Flags Manager: _____

Customer Identification Approved? Yes No

Additional Action? Yes No

If additional action was taken, please describe the action and circumstances: _____

Signature of Red Flags Manager: _____

Date: _____