Barton Hills Mortgage LLC
Identity Theft Prevention Program (ITPP) under the FTC FACT Act Red Flags Rule

---

I. Firm Policy

Our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. We will do this by developing and implementing this written ITPP, which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

Rule: 16 C.F.R. § 681.1(d).

II. ITPP Approval and Administration

The broker of record with TXSML, Ashley Hall has approved this initial ITPP. Ashley Hall is the designated identity theft officer and is responsible for the oversight, development, implementation and administration (including staff training and oversight of third party service providers of ITTP services) of this ITPP.

Rule: 16 C.F.R. § 681.1(e) and Appendix A, Section VI.(a).

III. Relationship to Other Firm Programs

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information, including our policies and procedures under Regulation S-P, [and] our CIP and red flags detection under our AML Compliance Program in the formulation of this ITPP, and modified either them or this ITPP to minimize inconsistencies and duplicative efforts. All customer records are retained for at least 3 years via digital media that is stored in a locked fire-proof safe. All hard documents are disposed via licensed document shredding service.

Rule: 16 C.F.R. § 681.1, Appendix A, Section I.

IV. Identifying Relevant Red Flags

To identify relevant identity theft Red Flags, our firm assessed these risk factors: 1) the types of covered accounts it offers, 2) the methods it provides to open or access these accounts, and 3) previous experience with identity theft. Our firm also considered the sources of Red Flags, including identity theft incidents our firm has experienced, changing identity theft techniques our firm thinks likely, and applicable supervisory guidance. In addition, we considered Red Flags from the following five categories (and the 26 numbered examples under them) from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to our firm and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist, but a way to help our firm think through relevant red flags in the context of our business. Based on this review of the risk factors, sources, and FTC examples of red flags, we have identified our firm's Red Flags, which are contained the first column ("Red Flag") of the attached "Red Flag Identification and Detection Grid" ("Grid").

Rule: 16 C.F.R. § 681.1(d)(2)(i) and Appendix A, Section II.

V. Detecting Red Flags

We have reviewed our covered accounts, how we open and maintain them, and how to detect Red Flags that may have occurred in them. Our detection of those Red Flags is based on our methods of getting information about applicants and verifying it under our CIP of our AML compliance procedures, authenticating customers who access the accounts, and monitoring transactions and change of address requests. For opening covered accounts, that can include getting identifying information about and verifying the identity of the person opening the account by using the firm's CIP. For existing covered accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of changes of address, reviewing credit report in depth to detect any inconsistencies. Those inconsistencies may include Hawk Alerts, unmatching social security number, address discrepancies, irregularity of accounts opened or closed. Based on this review, we have included in the second column ("Detecting the Red Flag") of the attached Grid how we will detect each of our firm's identified Red Flags.

Rule: 16 C.F.R. § 681.1(d)(2)(ii) and Appendix A, Section III.

VI. Preventing and Mitigating Identity Theft

We have reviewed our covered accounts, how we open and allow access to them, and our previous experience with identity theft, as well as new methods of identity theft we have seen or foresee as likely. Based on this and our review of the FTC's identity theft

rules and its suggested responses to mitigate identity theft, as well as other sources, we have developed our procedures below to respond to detected identity theft Red Flags.

Procedures to Prevent and Mitigate Identity Theft

When we have been notified of a Red Flag or our detection procedures show evidence of a Red Flag, we will take the steps outlined below, as appropriate to the type and seriousness of the threat:

Applicants. For Red Flags raised by someone applying for an account:

1. Review the application. We will review the applicant's information collected for our application (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
2. Get government identification. If the applicant is applying in person, we will also check a current government-issued identification card, such as a driver's license or passport. If the applicant is submitting an electronic application via our Web site, we will use [*describe your Internet authentication methods; under Resources, above, see the Guidance on Authentication in an Internet Banking Environment-Federal Financial Institutions Examination Council's (FFIEC)*]. We will always ask for a copy of photo ID to be submitted with loan application package.
3. Seek additional verification. If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, we may also verify the person's identity through non-documentary CIP methods, including:
    a. Contacting the customer
    b. Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker [or] the Social Security Number Death Master File [or *list other sources*]
    c. Checking references with other affiliated financial institutions, or
    d. Obtaining a financial statement.
    e. Obtaining a social security verification disclosure to submit with underwriting file with the lender
4. Deny the application. If we find that the applicant is using an identity other than his or her own, we will deny the account and alert the Texas Savings and Loan to discuss any procedural actions that should follow. A Denial Notice will be mailed immediately.
5. Report. If we find that the applicant is using an identity other than his or her own, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and our clearing firm.
6. Notification. If we determine personally identifiable information has been accessed, we will prepare any specific notice to customers or other required notice

under state law. *[Note*: *See National Conference of State Legislators' listing of state notification requirements (This site may not be updated or comprehensive. Each firm is responsible to research all applicable state requirements. State and local laws and regulations are not uniform. All broker-dealers must have policies and procedures reasonably designed to prevent and detect violations of the laws and regulations of the jurisdictions in which they operate.)]*

Access seekers. For Red Flags raised by someone seeking to access an existing customer's account:

1. Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Check with the customer. We will contact the customer using our CIP information for them, describe what we have found and verify with them that there has been an attempt at identify theft.
3. Heightened risk. We will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a customer's lost wallet, mail theft, a data security incident, or the customer's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.
4. Check similar accounts. We will review similar accounts the firm has to see if there have been attempts to access them without authorization.
5. Collect incident information. For a serious threat of unauthorized account access we may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:
    a. Firm information (both introducing and clearing firms):
        i. Firm name and CRD number
        ii. Firm contact name and telephone number
    b. Dates and times of activity
    c. Securities involved (name and symbol)
    d. Details of trades or unexecuted orders
    e. Details of any wire transfer activity
    f. Customer accounts affected by the activity, including name and account number, and
    g. Whether the customer will be reimbursed and by whom.
6. Report. If we find unauthorized account access, we will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. We may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to our FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and our clearing firm.
7. Notification. If we determine personally identifiable information has been accessed that results in a foreseeable risk for identity theft, we will prepare any specific notice to customers or other required under state law. [*see note at 6, under "Applicants" above]*
8. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure

that our response to a data breach does not limit or eliminate our insurance coverage.

9. Assist the customer. We will work with our customers to minimize the impact of identity theft by taking the following actions, as applicable:
    a. Offering to change the password, security codes or other ways to access the threatened account;
    b. Offering to close the account;
    c. Offering to reopen the account with a new account number;
    d. Not collecting on the account or selling it to a debt collector; and
    e. Instructing the customer to go to the FTC Identity Theft Web Site to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Rule: 16 C.F.R. § 681.1(d)(iii) and Appendix A, Section IV.

VII. Internal Compliance Reporting

Our firm's staff who are responsible for developing, implementing and administering our ITPP will report at least annually to our [Board *or* committee *or* designated member of senior management] on compliance with the FTC's Red Flags Rule. The report will address the effectiveness of our ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, service provider arrangements, significant incidents involving identity theft and management's response and recommendations for material changes to our ITPP. A checklist is required in every loan file to insure that the necessary items were reviewed and we are diligent in compliance.

Rule: 16 C.F.R. § 681.1, Appendix A, Section VI.(b).

VIII. Updates and Annual Review

Our firm will update this plan whenever we have a material change to our operations, structure, business or location or to those of our clearing firm, or when we experience either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. Our firm will also follow new ways that identities can be compromised and evaluate the risk they pose for our firm. In addition, our firm will review this ITPP annually, on [*date*], to modify it for any changes in our operations, structure, business, or location or substantive changes to our relationship with our clearing firm.

Rule: 16 C.F.R. § 681.1 (d)(2)(iv) and Appendix A, Sections V. and VI. (a) & (b).

IX. Approval

Approve the firm's ITPP by signing below.

I approve this ITPP as reasonably designed to enable our firm to detect, prevent and mitigate identity theft.

Rule: 16 C.F.R. § 681.1 (e)(1)&(2) and Appendix A, Section VI.(a).

Signed: ASHLEY HALL

Title: BROKER

Date: JANUARY 1 2010

ATTACHMENT: Red Flag Identification and Detection Grid (Grid)

BARTON HILLS MORTGAGE

Red Flag Identification and Detection Grid

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
1. A fraud or active duty alert is included on a consumer credit report.	We will verify that the fraud or active duty alert covers an applicant or customer and review the allegations in the alert.
2. A notice of credit freeze is given in response to a request for a consumer credit report.	We will verify that the credit freeze covers an applicant or customer and review the freeze
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	We will verify that the notice of address or other discrepancy covers an applicant or customer and review the address discrepancy.
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	We will verify that the consumer credit report covers an applicant or customer, and review the degree of inconsistency with prior history.
Category: Suspicious Documents	
5. Identification presented looks altered or forged.	Our staff who deal with customers and their supervisors will scrutinize identification presented in person to make sure it is not altered or forged.
6. The identification presenter does not look like the identification's photograph or physical description.	Our staff who deal with customers and their supervisors will ensure that the photograph and the physical description on the identification match the person presenting it.
7. Information on the identification differs from what the identification presenter is saying.	Our staff who deal with customers and their supervisors will ensure that the identification and the statements of the person presenting it are consistent.
8. Information on the identification does not match other information our firm has on file for the presenter, like the original account application, signature card or a recent check.	Our staff who deal with customers and their supervisors will ensure that the identification presented and other information we have on file from the account, such as photo ID, bank statements, paystubs/W2 are consistent.
9. The application looks like it has been altered, forged or torn up and reassembled.	Our staff who deal with customers and their supervisors will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled. If there is a suspicion a verification will be obtained via third party.

Category: Suspicious Personal Identifying Information	
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as an address that does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is listed on the Social Security Administration's (SSA's) Death Master File.	Our staff will check personal identifying information presented to us to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File. If we receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match.
11. Inconsistencies exist in the information that the customer gives us, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	Our staff will check personal identifying information presented to us to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables.
12. Personal identifying information presented has been used on an account our firm knows was fraudulent.	Our staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Our staff will validate the information presented when opening an account by looking up addresses on the Internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services
14. The SSN presented was used by someone else opening an account or other customers.	Our staff will compare the SSNs presented to see if they were given by others opening accounts or other customers.
15. The address or telephone number presented has been used by many other people opening accounts or other customers.	Our staff will compare address and telephone number information to see if they were used by other applicants and customers,
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	Our staff will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded.
17. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	Our staff will authenticate identities for existing customers by asking challenge questions that have been prearranged with the customer and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.