



Correspondent Lender Red Flag/Identity Theft Prevention Program Attestation

Federal regulations require that all financial institutions and their affiliates create an identity theft prevention program in accordance with the Red Flag Guidelines, which are part of the Fair and Accurate Credit Transaction (FACT) Act. The written program is designed to detect, prevent, and mitigate identity theft in connection with originating, processing, underwriting, and closing a mortgage loan.

Covered accounts include, but are not limited to:

- Consumer Loans (including mortgages and credit cards)
- Business Loans
- Checking and Savings accounts
- Trust accounts

Financial Institutions which initiate transactions on behalf of Wintrust Mortgage Corporation (WMC) are required to comply with WMC's Identity Theft Prevention Program. To be compliant, a Correspondent Lender must develop and implement reasonable policies and procedures to:

- Identify relevant Red Flags for the mortgage loan products that the Correspondent Lender offers, and incorporate those Red Flags into its Program
- Have processes in place to detect Red Flags that have been incorporated into the Program
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
- Ensure the program is updated and reviewed periodically to reflect changes in risks to customers and to the safety and soundness of the financial institution

Upon request, the Correspondent Lender will provide copies of its Red Flag program to WMC for periodic review.

Each Correspondent Lender is required to attest to their compliance with the program by completing and signing this form. Correspondent Lenders which fail to certify their compliance may be excluded from doing business with WMC.



CORRESPONDENT LENDER INFORMATION

Correspondent Name: _____

Address: _____

City: _____

State: _____

Zip Code: _____

Phone: _____

Name of Correspondent representative completing this form: _____

Job Title: _____

CORRESPONDENT CERTIFICATION

The Correspondent Lender checks each box which applies. By checking a box, the Correspondent Lender certifies that the described Red Flag requirement is understood and is currently met for all transactions submitted to WMC for purchase.

Relevant Red Flags have been identified for the loans that Correspondent Lender submits to WMC

Identified Red Flags have been incorporated into a formal Red Flag Program

Policies and procedures to detect the identified Red Flags have been defined and incorporated into the Program

Procedures are in place to respond appropriately to any detected Red Flags

The Red Flag Program will be periodically reviewed and updated to account for changes in risk

Signature: _____

Date: _____



Information Regarding a Red Flag Identity Theft Prevention Program

A Red Flag/Identity Theft Prevention Program (Program) must be adopted pursuant to the provisions of Section 114 of the Fair and Accurate Credit Transactions Act of 2003.

The Program should be designed to detect, prevent, and mitigate identity theft in connection with originating, processing, underwriting, and closing a mortgage loan. The Program must include reasonable policies and procedures to:

- Identify relevant Red Flags for the loans that are offered or maintained, and incorporate those Red Flags into the Program
- Detect Red Flags including, but not limited to the Categories of Red Flags listed herewith
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
- Ensure the Program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of the organization from identity theft
- Determine that all relevant service providers have appropriate controls in place
- Ensure that the Board or Executive Management (as appropriate) approve the written program and review periodic updates, at least annually, as to the adequacy and effectiveness of the Program.



RED FLAGS

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A Fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy.
4. 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:
 - a. A recent and significant increase in the volume of inquiries.
 - b. An unusual number of recently established credit relationships.
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that as closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. 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.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
11. 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.
12. 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:
 - a. The address on an application is the same as the address provided on a fraudulent application; or
 - b. The phone number on an application is the same as the number provided on a fraudulent application.



13. 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:
 - a. The address on an application is fictitious, a mail drop, or prison, or
 - b. The phone number is invalid, or is associated with a pager or answering service.
14. The SSN provided is the same as that submitted by other persons opening an account or other customers.
15. 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.
16. 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.
17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.
18. 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.

Unusual Use of, or Suspicious Activity Related to the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or cell phone, or for the addition of authorized users on the account.
20. A new revolving credit account is used in a manner commonly associated with known patterns or fraud patterns. For example:
21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is for example
 - a. Nonpayment when there is no history of late or missed payments;
 - b. A material increase in the use of available credit;
 - c. A material change in purchasing or spending patterns;
 - d. A material change in electronic fund transfer patterns in connection with a deposit account; or
 - e. A material change in telephone call patterns in connection with a cellular phone account.
22. 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).
23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.



24. The financial institution or creditor is notified that the customer is not receiving paper account statements.
25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.