RED FLAGS RULES COMPLIANCE

BANKERS ADVISORY

1. Compliance Program Overview
2. Terminology
3. Red Flag Detection & Response
4. Risk Assessment & Mitigation
5. Information Security
6. Consumer Privacy
7. Fair & Accurate Credit Transactions Act
8. Fair Credit Reporting Act
9. U.S.A. Patriot Act
10. Vendor Management

Roles & Responsibilities of Senior Management

1. *Reviewing and approving the company's Red Flag Identity Theft Plan and recommending updates or changes*
2. *Monitor changes to federal laws and mandates to ensure the company has the tools and resources to remain compliant*
3. *Providing guidance and assistance to the Compliance Officer charged with administering the program*
4. *Review audit reports and results of regulatory examinations*
5. *Review the company's response to incidents*
6. *Assess overall effectiveness on a periodic basis*

Roles & Responsibilities of the Compliance Officer

1. *Development and updating of the policy guide*
2. *Overall administering of the program*
3. *Development and delivery of employee training*
4. *Creating of the list of red flags*
5. *Assigning the level of risk to each red flag*
6. *Development of forms and recordkeeping materials*
7. *Coordination of audit functions*
8. *Reporting results of audits to senior management*
9. *Ensuring related policy and procedures are compliant, including*:

    - *Consumer privacy notice*
    - *Information security policy*
    - *Vendor management*

LEGAL REQUIREMENTS OF FACTA, SECTIONS 114 & 315

The Company must ensure that legal requirements are met in accordance with Sections 114 & 315 of FACTA. Summarized are the compliance obligations:

1. *The filing of Suspicious Activity Reports (SAR) in accordance with the regulation and applicable supervisory agency*
2. *Complying with prohibitions of FACTA regarding the sale, transfer, and placement for collection of certain debts resulting from identity theft*
3. *Implementing any requirements regarding the circumstances under which credit may be extended when the company detects a fraud or active duty alert*
4. *Implementing any requirements for furnishers of information to consumer reporting agencies, such as to correct or update inaccurate or incomplete information, and not to report information that the furnisher has reasonable cause to believe is inaccurate*

Training

Training is required for all employees. Training shall be completed annually and include updated information and requirements for the mortgage industry and apply to employees required to complete follow-through steps for red flag detection, response and mitigation.

Quality Control

Management is required to ensure that the pre-funding and post-funding quality control file reviews include a step to determine if the requirements of the Red Flags identity theft plan are met. Any exceptions noted in QC findings report shall require remediation and management response.

Auditing

Management must ensure that the internal controls and procedures established under the Red Flags Identity Theft plan to be tested at least annually by internal or external auditors, as applicable.

Identity Theft & Identifying Information

Identity theft *is a fraud committed or attempted Licensee identifying information of another person without authority.*

Identifying information *means any name or number that may be used (alone or in conjunction with any other information) to identify a specific person including the following:*

- *Name*
- *Social Security Number*
- *Date of Birth*
- *Official State or Government Issued Drivers License or ID*
- *Alien Registration Number*
- *Employer or Tax Payer ID Number*

Creditors

Organizations that regularly extend, renew or continue credit

Companies that make arrangements to extend, renew or continue credit

Assignees of companies who extend, renew, continue credit

Examples are:

- *Finance Companies*
- *Utility Companies*
- *Automobile Dealers*
- *Telecommunication Companies*
- *Mortgage Brokers*
- *Mortgage Lenders*

Financial Institutions

Banks, thrifts, credit unions and entities that hold a "transaction account" where a consumer can make payments, drafts or transfers.

Examples are:

- *Checking & Savings accounts*
- *Broker accounts where consumers can write checks*

Address Discrepancies

Notices sent to lenders by credit agencies informing the lender of a substantial difference between the info provided on the request order form with the agency's database.

Mandatory response steps include cross-checking data, verifying directly with the consumer and submitting a confirmation to the credit agency.

Covered Accounts

Credit cards, checking/savings accounts, car loans, cell phone service, utilities, margin accounts and mortgage loans.

Incident Response

Reporting of an information security breach, suspicious activity or red flag alert which cannot be cleared

Identity Theft Report

A report that alleges an identity theft An official, valid report filed by a consumer with an appropriate Federal, State, or local law enforcement agency

Identification of Red Flags

Red flags apply to covered accounts that include new or existing customer information accessed by the creditor or accessed by third parties. Red flags are often discovered by cross-checking telephone directories, public or internet sources. Listed are the types of sources which may contain a red flag:

- *Documents furnished by the consumer*
- *Documents furnished by transaction parties*
- *Documents furnished by employers or other income source*
- *Notices received from outside persons or entities in connection to the account being serviced*

Red Flags are generally identified on consumer reports as:

- *Alerts, notifications or warnings on the credit report*
- *Alerts noted on an SSN validation check*
- *Alerts noted on a Factual ID or Fraud-Check*

FTC List of 26 Red Flags

The Federal Trade Commission has identified "26 Red Flags" to be used as a guide for drafting an internal policy. The FTC list is not to be used as a "checklist" and companies must list sources and examples that are specific to their business model.

1. *A fraud alert was indicated in the consumer report*
2. *Notice of a credit freeze in a consumer report*
3. *A consumer reporting agency provided notice of address discrepancy*
4. *Unusual credit activity, such as an increased # of accounts or inquiries*
5. *Documents provided for identification appear altered or forged*
6. *Photograph on ID inconsistent with appearance of customer*
7. *Information on ID inconsistent with information provided by customer*
8. *Information on ID, such as signature, inconsistent with information on file at financial institution*

FTC List of 26 Red Flags

9. *Application appearing forged, altered or destroyed and reassembled*

10. *Information on ID does not match any address in the consumer report, SSN has not been issued or appears on the SSN Administration's Death Master File*

11. *Lack of correlation between SS number range and date of birth*

12. *Personal identifying information associated with known fraud activity*

13. *Suspicious addresses supplied, such as a mail drop, prison, phone numbers associated with pagers or answering service*

14. *SS number provided matches info submitted by another customer*

15. *Address or phone number matches other applicants*

16. *Customer unable to supply identifying information in response to notification that the application is incomplete*

17. *Personal information inconsistent with information already on file at financial institution or creditor*

18. *Person opening account or customer unable to correctly answer challenging questions*

FTC List of 26 Red Flags

19. *Shortly after change of address, creditor receives request for additional users of account*

20. *Most of available credit used for cash advances, jewelry or electronics, plus customer fails to make first payment*

21. *Drastic change in payment patterns, use of available credit or spending patterns*

22. *An account that has been inactive for a lengthy time suddenly exhibits unusual activity*

23. *Mail sent to customer repeatedly returned as undeliverable despite ongoing transactions on active account*

24. *Financial institution or creditor notified that customer is not receiving paper account statements*

25. *Financial institution or creditor notified of unauthorized charges or transactions on customer's account*

26. *Financial institution or creditor notified that it has opened a fraudulent account for a person engaged in identity theft*

Address Discrepancies

The law requires immediate response to all notices of address discrepancy that is received from the credit reporting agency.

Upon receipt of such notice, it is the responsibility of the loan processor or underwriter to lender to

- ***a)*** *compare the information in the credit report provided by the agency and;*
- ***b)*** *verify the information in the credit report directly with the consumer.*

The law requires the Company to furnish a borrower's address to the credit agency after the processor or underwriter reasonably confirms accuracy to the credit agency.

Accuracy of Information from Credit Agency Reports

The Red Flags Program sets forth a policy that all credit reports and additional investigative reports be cross referenced for accuracy.

Should there be a discrepancy in a borrower's address or other identifying information from one consumer report to an additional report, all steps and procedures must be followed.

The response, request for borrower explanations and other mitigation must be separately applied to each consumer report ordered.

The lender may inform applicants that they can dispute the accuracy of credit information directly through the credit reporting agency.

SOCIAL SECURITY VALIDATION

The lender requires a Social Security validation from a minimum of at least one consumer credit agency or factual investigation service. Validation of SSN must be from authorized sources that obtain information from the Social Security Administration.

FACTUAL ID REPORTS

The lender's underwriting procedures must conform to the investor or agency standards and a factual ID ordered, if applicable, with the resulting score included in the file.

FRAUD CHECKS

A Fraud Check can be ordered on a predetermined percentage of applications for a specific loan program, new loan originator, wholesale brokers, etc. in accordance with the plan. The score of a resulting Fraud check should be included in the file.

Alerts, Warnings from a Consumer Reporting Agency

The law requires immediate response to all alerts and warnings received by a credit agency. Reports may consist of a tri-merge credit report, Factual ID or Fraud Check report. The following examples are consistent with the types of red flags previously noted by the FTC:

1. *A fraud or active duty alert is included with a credit report.*
2. *The credit agency provides a notice of credit freeze in response to a request for a consumer report.*
3. *The credit report provides a notice of address discrepancy.*
4. *The credit report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:*

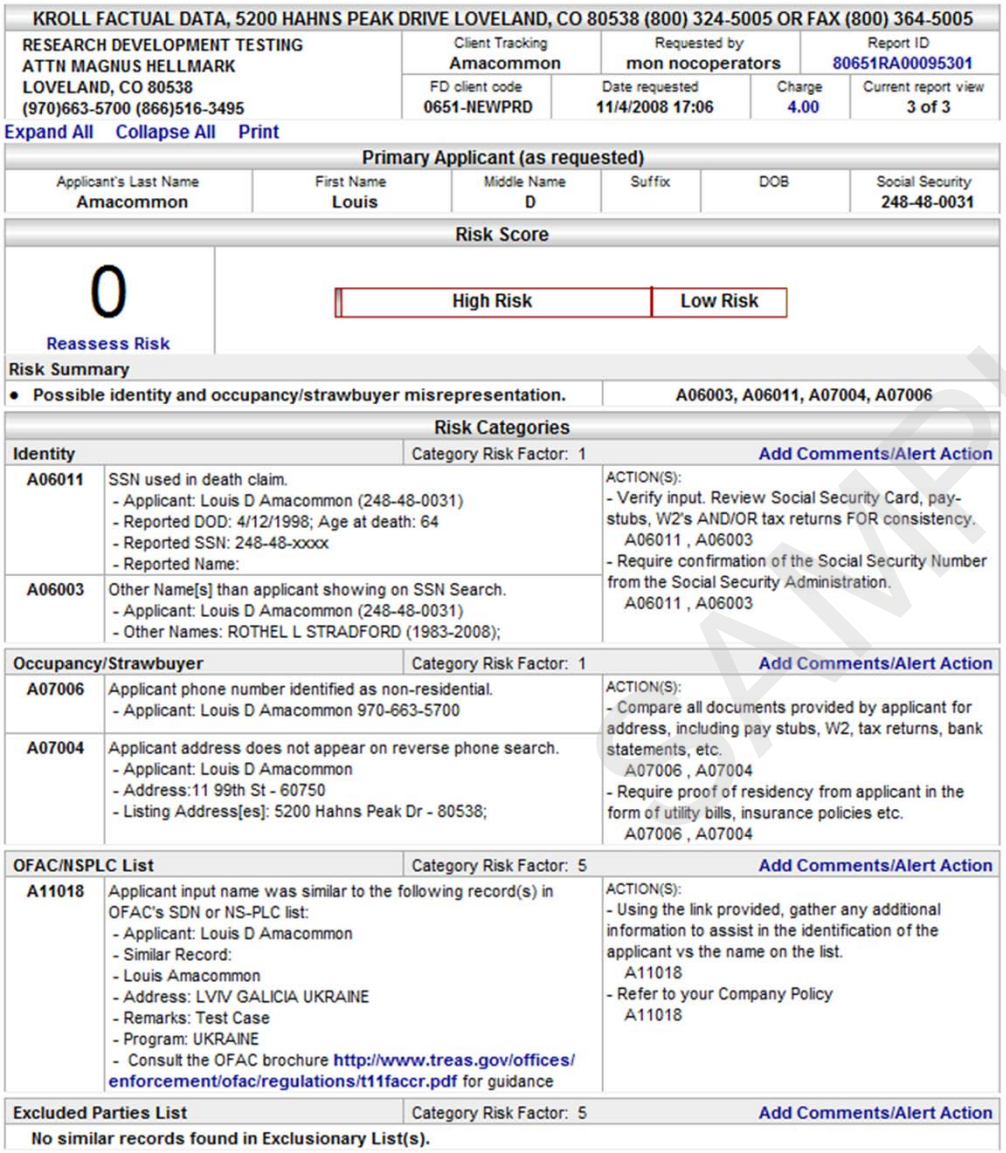
    - *A recent and significant increase in the volume of inquiries*
    - *An unusual number of recently established credit relationships*
    - *A material change in the use of credit, especially with respect to recently established credit relationships*
    - *An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor*

Procedures for Mitigating Alerts from a Credit Agency

Upon receipt of a consumer report that contains an initial, extended, or active duty alert, the lender must re-verify the identity of the customer. In addition to the company's requirements for ID information under the USA Patriot Act, the lender should request at least one additional piece of verification. If the alert contains instructions to contact the consumer before taking any action on the request, then the processor must contact the consumer for an explanation.

The lender's employee should document the Red Flags Checklist or comment sheet in the loan file or LOS system with the completed actions or steps. Additionally, the submitted additional verification by the borrower should be indicated. Permission should be granted by a supervisor or the compliance officer to continue processing any loan application prior to the mitigation of the red flag.

Procedures for Mitigating Alerts from a Credit Agency



KROLL FACTUAL DATA, 5200 HAHNS PEAK DRIVE LOVELAND, CO 80538 (800) 324-5005 OR FAX (800) 364-5005

RESEARCH DEVELOPMENT TESTING
ATTN MAGNUS HELLMARK
LOVELAND, CO 80538
(970)663-5700 (866)516-3495

Client Tracking	Requested by	Report ID
Amacommon	mon nocoperators	80651RA00095301

FD client code	Date requested	Charge	Current report view
0651-NEWPRD	11/4/2008 17:06	4.00	3 of 3

Expand All Collapse All Print

Primary Applicant (as requested)

Applicant's Last Name	First Name	Middle Name	Suffix	DOB	Social Security
Amacommon	Louis	D			248-48-0031

Risk Score

0

Reassess Risk

High Risk | Low Risk

Risk Summary

• Possible identity and occupancy/strawbuyer misrepresentation.	A06003, A06011, A07004, A07006

Risk Categories

Identity — Category Risk Factor: 1 — Add Comments/Alert Action

A06011	SSN used in death claim. - Applicant: Louis D Amacommon (248-48-0031) - Reported DOD: 4/12/1998; Age at death: 64 - Reported SSN: 248-48-xxxx - Reported Name:	ACTION(S): - Verify input. Review Social Security Card, pay-stubs, W2's AND/OR tax returns FOR consistency. A06011 , A06003 - Require confirmation of the Social Security Number from the Social Security Administration. A06011 , A06003
A06003	Other Name[s] than applicant showing on SSN Search. - Applicant: Louis D Amacommon (248-48-0031) - Other Names: ROTHEL L STRADFORD (1983-2008);	

Occupancy/Strawbuyer — Category Risk Factor: 1 — Add Comments/Alert Action

A07006	Applicant phone number identified as non-residential. - Applicant: Louis D Amacommon 970-663-5700	ACTION(S): - Compare all documents provided by applicant for address, including pay stubs, W2, tax returns, bank statements, etc. A07006 , A07004 - Require proof of residency from applicant in the form of utility bills, insurance policies etc. A07006 , A07004
A07004	Applicant address does not appear on reverse phone search. - Applicant: Louis D Amacommon - Address:11 99th St - 60750 - Listing Address[es]: 5200 Hahns Peak Dr - 80538;	

OFAC/NSPLC List — Category Risk Factor: 5 — Add Comments/Alert Action

A11018	Applicant input name was similar to the following record(s) in OFAC's SDN or NS-PLC list: - Applicant: Louis D Amacommon - Similar Record: - Louis Amacommon - Address: LVIV GALICIA UKRAINE - Remarks: Test Case - Program: UKRAINE - Consult the OFAC brochure http://www.treas.gov/offices/enforcement/ofac/regulations/t11faccr.pdf for guidance	ACTION(S): - Using the link provided, gather any additional information to assist in the identification of the applicant vs the name on the list. A11018 - Refer to your Company Policy A11018

Excluded Parties List — Category Risk Factor: 5 — Add Comments/Alert Action

No similar records found in Exclusionary List(s).

Factual ID uses a cutting-edge risk assessment engine to comprehensively detect potential identity theft and misrepresentation

← **Risk Score**
← **Risk Summary**

← **Red Flags / Alerts**
← **Action items**

← **Phone # and address discrepancies**

← **Incorporate custom exclusionary lists for names known to be associated with fraud; also include names from various watch lists (FBI, OFAC, etc)**

Procedures for Mitigating Alerts from a Credit Agency

Risk Categories			
Identity	Category Risk Factor: 1		Add Comments/Alert Action
A06011	SSN used in death claim. - Applicant: Louis D Amacommon (248-48-0031) - Reported DOD: 4/12/1998; Age at death: 64 - Reported SSN: 248-48-xxxx - Reported Name:	ACTION(S): - Verify input. Review Social Security Card, pay-stubs, W2's AND/OR tax returns FOR consistency. A06011 , A06003 - Require confirmation of the Social Security Number from the Social Security Administration. A06011 , A06003	
A06003	Other Name[s] than applicant showing on SSN Search. - Applicant: Louis D Amacommon (248-48-0031) - Other Names: ROTHEL L STRADFORD (1983-2008);		
Occupancy/Strawbuyer	Category Risk Factor: 1		Add Comments/Alert Action
A07006	Applicant phone number identified as non-residential. - Applicant: Louis D Amacommon 970-663-5700	ACTION(S): - Compare all documents provided by applicant for address, including pay stubs, W2, tax returns, bank statements, etc. A07006 , A07004 - Require proof of residency from applicant in the form of utility bills, insurance policies etc. A07006 , A07004	
A07004	Applicant address does not appear on reverse phone search. - Applicant: Louis D Amacommon - Address:11 99th St - 60750 - Listing Address[es]: 5200 Hahns Peak Dr - 80538;		

+	Applicants (as requested)		
+	Subject Property (as requested)		
-	Social Security Number Search Results		
1	Louis D Amacommon 248-48-0031		
Issuance SSN 248-48-0031 was issued prior to 1951 in South Carolina			
Name	**Address**	**Record Date**	**Reported DOB**
ROTHEL L STRADFORD	1668 DUCKWOOD Rd LANCASTER, SC 29720	7/1994 - 10/2008	2/ 2/ 1934
JOSE LANDSAFE	10 DOWN HI FREMONT, CA 94536	6/2008 - 10/2008	
LEE KYACOMMON	4093 LEAD ADDRESS Rd WAYNE, PA 19087	5/2008 - 9/2008	
JIMMY BIGSHOT	123 TEST EDED GLENDORA, CA 91741	8/2007 - 3/2008	
WILLIAM S FRAZIER	1517 E 8TH St STOCKTON, CA 95206	9/2006 - 9/2007	
LOUIS P AMACOMMON	11 99TH St TOMMORROW, IL 60750	8/2000 - 8/2007	5/ 1/ 1901

-	Reverse Phone Search			
1	Louis D Amacommon 970-663-5700			
Name	**Address**		**Listing Type**	**Phone Type**
Kroll Factual Data	5200 Hahns Peak Dr Loveland, CO 80538		Business	Landline

Automated detection of 20 red flags, including address discrepancies, suspicious addresses and phone numbers, plus SSN problems:

- **Reported deceased**
- **Associated with other name(s)**
- **Issuance discrepancies**
- **No correlation to name/ DOB**

← **SSN history**

← **Reverse phone search results**

Presentation of Suspicious Documents

The lender should require immediate response to all discrepancies and suspicious information found on documents furnished by the loan applicants or third parties. The following examples are consistent with the types of red flags previously noted by the FTC:

1. *Documents provided for identification appear to have been altered or forged.*
2. *The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.*
3. *Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.*
4. *Other information on the identification is not consistent with readily accessible information that is on file with the company, such as a signature card or a recent check.*
5. *An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.*