GETTING READY - THINGS TO CONSIDER

Risk Assessment Examples of Red Flags

The "Red Flag" Rules identify five categories of Red Flags and provide twenty-six examples.

Categories of Red Flags

- Alerts, notifications or other warnings received from consumer reporting agencies or service providers;
- Presentation of suspicious documents;
- Presentation of suspicious personal identifying information;
- Unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft or law enforcement authorities.

Risk Factors

A financial institution or creditor subject to the "Red Flag" Rules should consider the following factors in identifying relevant red flags for covered accounts, as appropriate.

- The types of covered accounts it offers or maintains;
- The methods it provides to open its covered accounts;
- The methods it provides to access its covered accounts; and
- Its previous experiences with identity theft.

Sources of Red Flags

Financial institutions and creditors subject to the "Red Flag" Rules should incorporate relevant red flags from sources such as:

- Incidents of identity theft that the financial institution or creditor has experienced;
- Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and
- Applicable supervisory guidance.

Examples of Red Flags

An Appendix to the Red Flag Rules includes twenty-six examples of red flags for covered accounts, including the following:

- A fraud or active duty alert on a consumer report;
- A notice of "credit freeze" on a consumer report;
- A consumer reporting agency providing a notice of address discrepancy;
- Documents provided by the consumer that appear to have been altered or forged;
- The failure of the consumer opening a covered account to provide all required personal identifying information on an application;
- The use of a covered account in a manner that is not consistent with established patterns of activity on the account;
- The return of mail sent to the consumer as undeliverable, although transactions continue to be conducted in connection with the account;
- Use of an account that has been inactive for an unreasonably lengthy period of time; and
- Notice from the consumer or law enforcement that identity theft has occurred.

Possible Responses to Red Flags

- Monitor a covered account for evidence of identity theft;
- Contact the customer;
- Change any passwords, security codes, or other security devices that permit access to a covered account;
- Reopen a covered account with a new account number;
- Not open a new covered account;
- Close an existing covered account;
- Notify law enforcement; or
- Determine no response is warranted.

Checklist of Things to Consider

☐ Review the regulatory requirements;

☐ Determine applicability of the regulatory requirements to the accounts maintained and offered;

☐ Conduct an assessment to determine where and how personal identifying information is maintained;

☐ Develop and conduct a risk assessment;

- ☐ Evaluate any existing identity theft prevention and anti-fraud programs;
- ☐ Assess red flags currently employed for appropriate risk levels and currency;
- ☐ Evaluate red flag monitoring systems and methodologies; and
- ☐ Evaluate the training program established for key relevant personnel.