



R E D
F L A G
PROVISIONS
2 0 0 9

IDENTITY THEFT RED FLAG FAQs

PROVIDED TO YOU BY



PREPARED BY
EDUARD GOODMAN, J.D.,LL.M.
CHIEF PRIVACY OFFICER
IDENTITY THEFT 911, LLC

Red Flag Provisions**CONTENTS**

- I. What are people referring to when they say “Red Flag Provisions”?
PAGE 3
- II. What are these Red Flag Provisions all about?
PAGE 3
- III. Do we have to do this?
PAGE 3
- IV. Why do we have to do this?
PAGE 4
- V. Who is making us do this?
PAGE 4
- VI. What do I actually have to do as an institution?
And how do I actually do it?
PAGE 5
- VII. Is there a “Master List” of Red Flags that we can pull from in order to
determine which ones apply to us and our business?
PAGE 6
INTERNAL RED FLAG SOURCES
EXTERNAL RED FLAG SOURCES
- VIII. How does one “prevent and mitigate” identity theft once Red Flags
are actually discovered?
PAGE 10
- IX. When do I have to have my program implemented by?
PAGE 11
- X. Once we’re done writing our program and implementing it, we’re
done, right?
PAGE 12

LEGAL NOTICE: The text contained herein is for informational purposes only and should not be relied on for final legal determinations and/or evaluations. Nothing in this document shall be construed as the rendering of legal advice. Questions or concerns of a legal nature should be directed to legal counsel qualified in the requisite areas of the law and licensed in the appropriate jurisdiction(s).

COPYRIGHT NOTICE: © 2009. All Rights Reserved. The reproduction, copying, or redistribution for commercial purposes of any materials or design elements of this document is strictly prohibited without the express written permission of Identity Theft 911.

Red Flag Provisions**I.****What are people referring to when they say “Red Flag Provisions”?**

There has been a lot of talk lately about the new “Red Flag Provisions” and the looming deadlines and responsibilities associated with them. When people are referring to the Red Flag Provisions, they are really referring a set of requirements and guidelines known officially as the “Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003”. As this can be a mouthful, the short form way to refer to this is to simply call them the Red Flag Provisions. A “Red Flag” really is just defined as:

“a pattern, practice, or specific activity that indicates the possible existence of identity theft.”

II.**What are these Red Flag Provisions all about?**

The costs of identity theft and fraud in America are astounding. In the past, most of the burden in preventing identity theft was carried by the consumer. The simple fact is that every day, all over the country, businesses unintentionally help contribute to fraudulent activities by granting credit to identity thieves. Failing to recognize the signs or “Red Flags” that someone may not actually be who they say they are puts both the business and consumer in a vulnerable situation; one where they are both more susceptible to falling victim to an identity thief simply because the business had no basic procedures and processes in place to help recognize identity thieves.

The Red Flag Provisions are meant to shift the burden of preventing identity theft from the consumer to businesses that issue credit. They require that all businesses with certain types of accounts (referred to as “Covered Accounts”) put a plan in place to help recognize the red flags/warning signs associated with fraud and identity theft. The plans must be designed to *“detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or existing accounts.”* The plan must also be created with the expectation that it will need to be continuously evaluated and revised in order to keep up with identity theft trends and the company’s own experiences with identity related fraud.

III.**Do we have to do this?**

That depends upon whether or not your business maintains “Covered Accounts.” The Red Flag provisions define a Covered Account as being:

1. *“an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or*
2. *any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.”*

Red Flag Provisions

Whether or not your business or institution maintains “Covered Accounts” is for you to determine. A business will have to see if any of their practices or risks falls under the above definitions, and if so will be governed by these requirements.

It is important to note that even if your business has determined that it does NOT initially maintain covered accounts, the Red Flag Provisions necessitate that:

“Each financial institution and creditor must periodically determine whether it offers or maintains a ‘covered account.’”

Therefore, it is critical to periodically re-evaluate whether or not your business or institution maintains such accounts. Again, if it has been determined that your business or institution maintains covered accounts, then the Red Flag provisions will apply to you.

IV.**Why do we have to do this?**

Mistakenly granting credit to someone pretending to be someone else affects three parties:

1. the person (victim) who has had his/her identity stolen;
2. the company that erroneously grants credit; and
3. the consumer public.

The identity theft victim has to fight to restore their credit and good name, costing them lost time, productivity and money, not to mention the psychological stress. When the identity theft victim actually recognizes that erroneous charges were due to identity related fraud or when these charges go unpaid, it is the creditor who usually ends up taking the financial loss. This loss is then passed down to the consumer public who as result must pay higher costs for goods and services to make up for those losses. It’s a losing situation all the way around, except for the identity thief. The Red Flag Provisions are meant to help prevent these situations from occurring.

V.**Who is making us do this?**

The FACT Act was passed by Congress to amend and strengthen the Fair Credit Reporting Act (FCRA). In the FACT Act, §114 requires that “(t)he Federal banking agencies, the National Credit Union Administration, and the Commission shall jointly, with respect to the entities that are subject to their respective enforcement authority” establish procedures for recognizing possible instances of identity theft. These procedures were laid out in the Red Flag provisions, and are more specifically enacted by:

Red Flag Provisions

- Office of the Comptroller of Currency, Treasury (OCC);
- Board of Governors of the Federal Reserve System (Board);
- Federal Deposit Insurance Corporation (FDIC);
- Office of Thrift Supervision, Treasury (OTS);
- National Credit Union Administration (NCUA); and
- The Federal Trade Commission (FTC);
(Collectively these groups are referred to as “the Agencies”.)

VI.**What do I have to do as an institution? And how do I do it?**

The reality is that most large companies that extend credit in any way, shape or form already have extensive programs and processes in place to recognize fraud and spot identity thieves prior to granting credit. Large institutions and businesses tend to have internal fraud departments whose sole responsibility is to identify and fight fraud in order to protect their company. The motivation was not to protect the consumer, but to protect the company from losing money.

Most small and medium sized businesses don't have internal fraud departments: therefore, it is unlikely that they have put together processes and procedures to deal with identity related fraud. This is something that the average business has never thought of, even if the business has been a victim of identity theft. This is why the Red Flag provisions have been written so broadly. They are meant to allow an institution to set forth policies and procedures to specifically address their particular industry and business.

The Red Flag Provisions really outline four main elements of a company's Red Flag program. Essentially, the Program must include reasonable policies and procedures to:

1. Identify relevant Red Flags;
2. Detect Red Flags;
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
4. Ensure the Program (including the Red Flags determined to be relevant) is updated periodically to reflect changes in risks to customers and to the safety and soundness of the institution from identity theft.

As mentioned earlier, it is important to note that once you have a program set in place that you must periodically and continuously re-evaluate the plan to reflect new red flags and

Red Flag Provisions

threats. Whether you are putting together your initial program, or making changes to the program, every business that is required to:

1. *“Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors;*
2. *Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the Program;*
3. *Train staff, as necessary, to effectively implement the Program; and*
4. *Exercise appropriate and effective oversight of service provider arrangements.”*

If the business or institution is small, then the “board of directors” could simply be the business owner him/her self. Therefore, these basic requirements and administration of the program are not as complex as they seem. Please note that there is no true “one size fits all” approach to coming up with a program so some hard work may be needed to get your program implemented.

VII.

Is there a “Master List” of Red Flags that we can pull from to help determine which ones apply to us and our business?

INTERNAL RED FLAG SOURCES

Appendix J of the Red Flag provisions lays out two separate groupings or “sources” of Red Flags to look at. The first source listed in section II(b) of Appendix J indicates that financial and business institutions should incorporate relevant red flags from various sources of a more internal nature, such as:

1. *“Incidents of identity theft that the financial institution or creditor has experienced;*
2. *Methods of identity theft that the financial institution or creditor has identified that reflect changes in identity theft risks; and*
3. *Applicable supervisory guidance.”*

EXTERNAL RED FLAG SOURCES

Supplement A to Appendix J offers up more specific guidance on identifying red flags. It breaks down red flags into four (4) main sections or categories, which in total contains twenty-six (26) separate external red flags for consideration. The Sections are:

- Alerts, Notifications or Warnings from a Consumer Reporting Agency
- Suspicious Documents
- Suspicious Personal Identifying Information

Red Flag Provisions

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

The following Excerpt from Supplement A to Appendix J lays out all of the specifically enumerated Red Flags. Not all of these will apply to every business, but this should be a good starting point to help determine what specific red flags apply to your business:

"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, as defined in §41.82(b) of this part.*
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 was 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.*

Red Flag Provisions*Suspicious Personal Identifying Information*

10. *Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:*
 - a. *The address does not match any address in the consumer report; or*
 - b. *The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.*
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 a 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

Red Flag Provisions*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 a new, additional, or replacement card or a 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 of fraud patterns. For example:*
 - a. *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*
 - b. *The customer fails to make the first payment or makes an initial payment but no subsequent payments.*
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 the 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."*

Red Flag Provisions

As you can see from the rather extensive list provided, not all red flags apply to all businesses. For instance, some red flags are more applicable to certain institutions than others due to their size, complexity or type of service they provide. The decision as to whether ALL the above mentioned red flags or which specific red flags apply is up to each institution and business to identify. The choice is yours, as you understand your business and potential vulnerabilities better than anyone else. Do keep in mind that red flags should also be revisited on a regular basis along with your program.

VIII.

How does one “prevent and mitigate” identity theft once Red Flags are discovered?

Once a pre-identified set of red flags are spotted, then the business has a duty to prevent and mitigate any potential identity theft. This again sounds more complicated than it really is. All that is meant is that the program lays out some type of response to the problem. The Red Flag provisions provide suggested responses such as:

1. *“Monitoring a covered account for evidence of identity theft;*
2. *Contacting the customer;*
3. *Changing any passwords, security codes, or other security devices that permit access to a covered account;*
4. *Reopening a covered account with a new account number;*
5. *Not opening a new covered account;*
6. *Closing an existing covered account;*
7. *Not attempting to collect on a covered account or not selling a covered account to a debt collector;*
8. *Notifying law enforcement; or*
9. *Determining that no response is warranted under the particular circumstances.”*

The response simply means that a decision must be made by the institution as to which action or actions are warranted in a particular situation.

Red Flag Provisions**When do I have to have my program implemented by?**

The Deadline for compliance with the Red Flag provisions was November 1st, 2008. Unfortunately, it became quite clear that the vast majority of the 11 million+ businesses that these regulations applied to would NOT meet the November 1st, 2008 compliance deadline. So on October 22, 2008, the Federal Trade Commission (FTC) issued a press release regarding their delay on enforcement of the “Red Flag Rule”. Remember that the FTC is the federal agency charged with enforcing the “Red Flag Rule” and provisions as they apply to non-financial institutions (essentially all businesses with covered accounts other than banks, credit unions and the like).

In their press release, the FTC acknowledged the fact that many businesses needed additional time to properly implement their Red Flag Programs and that the FTC would be extending enforcement of the “Red Flag Rule” for six (6) months, or until May 1st, 2009. A new deadline of Nov. 1, 2009, has been set. However this *ONLY* applies to institutions that are regulated by the FTC and does not apply to those institutions where enforcement is carried out by another Federal authority such as:

- Office of the Comptroller of Currency, Treasury (OCC);
- Board of Governors of the Federal Reserve System (Board);
- Federal Deposit Insurance Corporation (FDIC);
- Office of Thrift Supervision, Treasury (OTS); or
- National Credit Union Administration (NCUA);

So it is important to note that if a company has not yet complied with these regulations, it would be best to put some type of program into place as quickly and efficiently as possible. The delayed enforcement of the Red Flag Rule by the FTC for the reason of allowing institutions with covered accounts to put a proper program into place simply underlines two important points:

1. Putting an Identity Theft Red Flag program into place should be a priority;
2. Once the Nov. 1, 2009 deadline has passed, the FTC will likely be scrutinizing companies that have no programs or have programs that are woefully inadequate and penalizing them as they have had additional time to meet compliance;

The best approach is to realize that: a functional but less than perfect plan implemented today is far better than a perfect plan that will implemented tomorrow. Remember, it is simply expected that the plan will be improved as time goes on as it must be revisited “periodically”.

What this means is that the best approach is to put SOMETHING into place, then work on refining it as time goes on. The key is to show any potential regulator that a clear effort is being made by the business or institution to comply with the Red Flag provisions. Remember

Red Flag Provisions

that the Red Flag provisions clearly state that the “Program must be tailored to the entity’s size, complexity and nature of its operations.” This means that every business or institution will have very different requirements. In the end compliance is met pretty simply but will require some work and analysis of how the company deals with “covered accounts” and what red flags should apply to the institution.

X.**Once we’re done writing our program and implementing it, we’re done, right?**

Wrong, businesses are required to periodically re-examine whether or not they maintain “covered accounts”, and the businesses and institutions should periodically update their plans. Again, the Red Flag provision offers vague suggestions on the factors used to re-evaluate a program:

Financial institutions and creditors should update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft, based on factors such as:

1. The experiences of the financial institution or creditor with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the financial institution or creditor offers or maintains; and
5. Changes in the business arrangements of the financial institution or creditor, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

Unfortunately, this is not a duty that is going away over time. Businesses and institutions that maintain “covered accounts” are expected to remain vigilant and dedicated to maintaining their program over the life of their company. Businesses and institutions will, as of November 1st, 2009, constantly be required to look at trends in identity theft, educate themselves about identity theft and fraud, learn from past mistakes and remain committed to their Identity Theft Program.

LEGAL NOTICE: The text contained herein is for informational purposes only and should not be relied on for final legal determinations and/or evaluations. Nothing in this document shall be construed as the rendering of legal advice. Questions or concerns of a legal nature should be directed to legal counsel qualified in the requisite areas of the law and licensed in the appropriate jurisdiction(s).

COPYRIGHT NOTICE: © 2009. All Rights Reserved. The reproduction, copying, or redistribution for commercial purposes of any materials or design elements of this document is strictly prohibited without the express written permission of Identity Theft 911.