



R E D
F L A G
S T E P S
2 0 0 9

SEVEN EASY STEPS TO CREATING AN IDENTITY THEFT RED FLAG PROGRAM

INCLUDING PROGRAM CONSIDERATIONS AND
EVALUATIONS



IOWA MUTUAL INSURANCE COMPANY

Built on Relationships, Dedicated to Service

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

CONTENTS

Introduction

PAGE 3

STEP 1 — DETERMINE “Coverage”

PAGE 4

STEP 2 — ADMINISTER the Program

PAGE 5

STEP 3 — IDENTIFY all Relevant Red Flags

PAGE 6

STEP 4 — DETECT Identity Theft

PAGE 10

STEP 5 — PREVENT Identity Theft

PAGE 13

STEP 6 — MITIGATE Identity Theft

PAGE 14

STEP 7 — REPEAT the process all over again (“Periodically”)

PAGE 15

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: © 2008. 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.

INTRODUCTION

In November of 2003, Congress passed the **Fair and Accurate Credit Transactions Act of 2003** ("FACT Act"), which was signed into law by President George W. Bush in December of 2003. The FACT Act was passed by Congress to amend and strengthen the Fair Credit Reporting Act ("FCRA") and to strengthen consumer rights regarding the integrity of credit data.

Under section 114, the FACT Act specifically 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 and guidelines are officially known as the **"Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003"** but have more commonly been referred to simply as "the Red Flag provisions."

The Red Flag provisions simply 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 plan must be designed to *"detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or existing accounts."*

The Red Flag provisions provide very loose guidance on the development of a plan for those institutions that the Red Flag provisions apply to. The Federal Trade Commission estimates that over 11 million businesses are covered under the Red Flag provisions. This means that the Red Flag provisions had to be drafted in an extremely broad manner. This is the only way that the Red Flag provisions would effectively provide guidance on the development of Red Flag programs for institutions that span a wide swath of industries and that vary in size from small, local mom and pop stores to large multinational corporations that do business in all fifty states.

The Red Flag provisions therefore do not contemplate a "one size fits all" approach to developing a plan. Instead the Red Flag provisions require that the *"Program must be tailored to the entity's size, complexity and nature of its operations."* Since there is no one size fits all approach, and since every business, industry and market segment will have its own specific considerations, this document is meant to help provide a very broad overview to developing a workable Identity Theft Red Flag program. This document is neither a template nor an instruction manual but more of an overall roadmap that can assist any organization, regardless of the nature, size or scope of that business.

STEP 1
DETERMINE “COVERAGE”

The first step to coming up with a Red Flag program is to find out, first and foremost, whether your business or institution is even required to have such a program. A business or institution is only required to have a Red Flag program if it maintains “Covered Accounts”. Covered Accounts are defined as:

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.”*

So when looking at accounts to determine whether they are “Covered Accounts” as defined above, a business or institution should take the following factors into consideration in order to make a firm determination as to whether or not they maintain Covered Accounts for purposes of developing a robust Red Flag program:

- i. The methods the business or institution provides to open accounts;
- ii. The methods the business or institution uses to access its accounts; and
- iii. The business’s/institution’s previous experience with identity theft;

If upon looking at BOTH the definition of a Covered Account and the three factors listed above it is determined that the business/institution maintains Covered Accounts, then a business or institution must develop and implement a written Red Flag program designed to detect, prevent and mitigate identity theft in connection with the opening of a “Covered Account.” The written program should be tailored to both the **size and complexity of the business or institution** as well as the **nature and scope of the operation**. To put it as simply as possible, the plan must contain “**reasonable policies and procedures**” to:

- i. **IDENTIFY** Red Flags for the covered accounts that the institution maintains and incorporate them into a Red Flag Program.
- ii. **DETECT** Red Flags that have been incorporated into the Program
- iii. **RESPOND** appropriately to any Red Flags that are detected in order to:
 - a. Prevent identity theft; and
 - b. Mitigate identity theft
- iv. **UPDATE** the program periodically to reflect changes in the risks to customers and to the safety and soundness of the institution from identity theft.

If, upon much reflection and evaluation, it is determined that a business/institution does NOT maintain covered accounts and is therefore not required to maintain a written identity theft Red Flag program then that business/institution can stop here. However, it is important to note that even a business/institution that does **not** maintain applicable covered accounts should still revisit this evaluation every 12-18 months to make a periodic determination as to whether or not it must create such a program at a later date.

STEP 2 ADMINISTER THE PROGRAM

In administering a Red Flag program, a business or institution really has five actions that they need to undertake.

First, a determination needs to be made as to who is going to be in charge of the program. If the business is small or a sole proprietorship, this determination could be very easy: The business owner or manager should be responsible for administering the program. If the business or institution is larger then there may not be just one person responsible but perhaps a team of people responsible for administering the program. Regardless of who is responsible, someone must be charged with overseeing and administering the program and a determination should be made regarding appointing someone for the responsible individual or team to report to on the program.

Second, once the responsible party or team in charge of the program has developed the initial program and put it into writing, that individual or team must obtain approval by the board of directors (if any) or an appropriate committee of the board. Obviously, if the business or institution is a sole proprietorship or small business, the owner or manager may be both the person responsible for being in charge of and giving approval of the Red Flag program.

Third, the responsible party must involve the board, committee or an employee at the senior level of management in the oversight, development, implementation and administration of the Red Flag program. The intent behind this is that a Red Flag program should not “exist in a vacuum” so to speak and there should be buy in by all relevant staff, from senior staff and management all the way down to the employees of the business or institution. Involvement by senior staff in the program is the first step to getting universal acceptance and adherence to any meaningful Red Flag program.

Fourth, once the program has been developed and implemented, all relevant staff should be trained and educated about the program. There is no sense in having a Red Flag program if no one knows about it or how to follow its protocols. Ongoing education and training on an annual basis is one of the best ways to ensure that a Red Flag program is a “living and breathing document” that doesn’t just collect dust on a shelf somewhere but that actually helps a business or institution avoid falling victim to and exposing consumers to identity theft.

Fifth, supervision is key. This means that the program should be administered internally within the institution, but also externally, with regard to any and all relevant vendors, service providers and strategic partners. A program is only as good as the adherence to that program by all parties at risk, and this includes suppliers and contractors. So be sure that as a business or institution you maintain proper oversight of the program and that anyone else that a business or institution works with ALSO adheres to the protocols of the program. Remember that if a vendor opens a new account for an identity thief on behalf of or as part of the products or services offered by a company or institution, that company or institution might be responsible for the fraudulent account and will likely face a loss as a result.

STEP 3 IDENTIFY ALL RELEVANT RED FLAGS

Each and every business or institution must take it upon itself to identify all of the RELEVANT Red Flags that apply to it. These Red Flags will vary from business to business and institution to institution. The type of business an institution is in as well as the way it carries out its business is extremely relevant to the specific Red Flags that a particular entity must mark as being relevant. The Red Flag Rules lay out 26 separate specific Red Flags, but a business or institution may add more, or only have certain ones that actually apply to its particular business. For instance an online business will have no need for certain Red Flags such as whether certain identification documents appear forged or altered since online businesses rarely if ever see or examine physical specimens of identification. However, a more traditional bricks and mortar business can and should scrutinize such documents when they appear altered or forged and this should become a relevant Red Flag for that business.

The Red Flags can be broken down into two separate categories. The first Category could be considered "INTERNAL RED FLAG SOURCES" while the second category would be considered "EXTERNAL RED FLAG SOURCES".

INTERNAL RED FLAG SOURCES require a business or institution to look inwards and reflect on and base these Red Flags on the following:

"(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 are laid out specifically in Supplement A to Appendix J of the Red Flag Regulations. This lays out twenty-six (26) specific Red Flags that business and institutions should consider when developing their own written Red Flag program. These External Red Flags are broken down into four (4) main sections which are:

- *Alerts, Notifications or Warnings from a Consumer Reporting Agency*
- *Suspicious Documents*
- *Suspicious Personal Identifying Information*
- *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. Remember though that not all of these will apply to every business or institution. However, these should be the ideal starting point to help and determine what specific Red Flags should be incorporated into a business's or institution's written program:

"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 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 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 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."*

By looking at the above enumerated Red Flags laid out in the Red Flag provisions it should be quite clear that not all Red Flags are universally applicable to all businesses. It is also important to note that this is not considered an exhaustive list and that other Red Flags based on an institution's or business's own experience with identity theft should also be added. Since the Red Flag provisions require that programs are to be reviewed and revised periodically it is important to revisit the applicable Red Flags to see if they continue to be relevant, or irrelevant depending upon the situation.

STEP 4

DETECT IDENTITY THEFT

The stated goal of the Red Flag provisions is that institutions and businesses should “detect, prevent and mitigate” identity theft in relation to the opening and maintenance of covered accounts. Detection is driven by taking the Red Flags deemed relevant to an institution or business (in STEP 3) and using tools and procedures applicable to the nature, scope and type of operation to spot those Red Flags.

It is important to note that training of staff on the Red Flags deemed relevant by the business or institution and methods of spotting those Red Flags is important. For instance if a member of a company’s sale staff processes applications for new accounts (in this case “covered accounts”) then obviously that sales staff member must be properly trained on the company’s or institution’s processes surrounding detection of Red Flags and must be educated on what the proper protocols should be.

Now the method and process of detection will vary from institution to institution and business to business. However there are really three main ways or processes that can be used to detect Red Flags deemed relevant by a business or institution. These are: (1) manual detection processes; (2) electronic detection processes; and (3) some combination of BOTH manual and electronic detection processes. Again, the type of process is going to be largely dependent upon the way a business or institution conducts its business and opens accounts.

Most smaller businesses where cost is an issue will likely utilize manual detection processes. This means that during the process of opening a covered account for an individual; manual steps are taken to try and assess the risk of fraud by looking at the relevant Red Flags. For example, a manual account application process would likely scrutinize various documents provided by an applicant. This means that the company should draw heavily from the sample Red Flags falling under the umbrella of “Suspicious Documents”. The individual taking and/or processing an application should be scrutinizing physical documents looking closely for certain specific enumerated Red Flags asking:

- *Do documents provided for identification appear to have been altered or forged?*
- *Is the photograph or physical description on the identification consistent with the appearance of the applicant or customer presenting the identification?*
- *Is other information on the identification inconsistent with information provided by the person opening a new covered account or customer presenting the identification?*
- *Is other information on the identification inconsistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check?*
- *Does an application appear to have been altered or forged, or gives the appearance of having been destroyed and reassembled?*

The above bulleted Red Flag examples are just some of the Red Flags that may apply to a specific business or institution. However, they are illustrative of manually detected Red Flags that require little training or expertise but that can still result in the prevention of identity fraud. The specific manual detection processes will vary greatly from business to business and institutions to institution but in the end the result should be the same, picking up on

suspicious activity that may be the precursor to the commission of the crime of identity theft.

Other institutions or businesses, depending on the manner in which they conduct business, may rely solely on electronic means of detection. For example, internet based businesses conducting E-commerce do not have the luxury of conducting manual Red Flag detection as they never physically come into contact with their customers. This means that these types of businesses must rely on more modern techniques and technology to help them detect relevant Red Flags for their business. While there are several service providers out there that allow businesses and institutions to run new account applicants through an electronic risk assessment process/service for a fee, there are other ways to detect relevant Red Flags using technology. For instance, by pulling an applicant's credit report from one, or better yet, all three of the credit bureaus, tools can be put into place to check the information provided by the bureaus electronically with the information provided by an applicant for the opening of a covered account. This simply involves establishing and putting into place the process and tools to pull credit files from the bureaus and then doing an information comparison.

Some of the enumerated Red Flags that can be checked using electronic data comparison, or even a combination of manual and electronic comparison would be:

- *Checking to see if 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.*
- *Determining whether personal identifying information provided by the customer is consistent with other personal identifying information provided by the customer. For example, if there is a lack of correlation between the SSN range and date of birth.*
- *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.*
- *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.*

- *The SSN provided is the same as that submitted by other persons opening an account or other customers.*
- *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.*

These above enumerated Red Flags are easily recognized using rudimentary electronic processes such as conducting checks across internal databases of customers as well as keeping up to date about common fraud addresses and geographic areas often utilized as drop houses. For example areas in Detroit, Michigan and Jamaica/the Bronx, in New York have long been recognized as a center for fraud and drop houses. While this doesn't mean that all applications for the opening of covered accounts originating from these locales are fraudulent, it does mean that applications originating from this geographic locations (and others) should be subject to higher scrutiny based on this prior and common knowledge surrounding the high propensity for identity fraud originating from these areas.

While some businesses and institutions may rely completely on manual processes and others may rely completely on electronic processes, the best and most robust method of detecting relevant Red Flags is to utilize some combination of both manual and electronic processes to spot potential Red Flags of Identity Theft.

STEP 5
PREVENT IDENTITY
THEFT

The key to preventing identity theft is to have proper protocols and procedures in place that allow the relevant personnel at a business or institution to know what to do to once they detect a potential Red Flag. Remember that just because a Red Flag is detected does NOT mean that there is an actual identity theft situation. It simply means that there may in fact be a situation and that the situation must be examined more closely.

Prevention is accomplished simply by recognizing when a Red Flag has been detected and putting secondary procedures into place to either: (a) Prevent the potential Identity Thief from opening a covered account with the business or institution; or (b) If the application is NOT actually fraudulent but legitimate, to allow it to go through and continue business as usual.

Prevention of identity theft requires that a business actually draft a procedure on what to do once a Red Flag has been detected. This may mean that the applicant is asked to provide secondary documentation that an Identity Thief would likely not have access to. This might involve bringing in a more senior level manager to scrutinize an application more closely. It might involve simply rejecting the application because, even if there is not certainty that the application is from an identity thief, it is not worth the money for the business or institution to take the risk. The appropriate process and procedure will really be completely up to each institution and will vary greatly depending on the amount of risk and what is at stake. For instance the process for a health spa account application will be drastically different from a credit application at an auto dealership or a bank that processes a home equity line of credit.

An important thing to remember when drafting the relevant processes and procedures is to realize that prevention of identity theft is something that benefits both the consumer AND the business or institution. While there may be a consumer out there who has had their identity stolen, in the end the business that allows an identity thief to open a covered account will be left with the bill once the account is determined to be fraudulent. This means that a business or institution has a vested interest in preventing fraudulent applications and opening of covered accounts because in the end they will be losing money as a result.

STEP 6
MITIGATE IDENTITY
THEFT

Mitigation of identity theft is really very closely tied to prevention. Mitigating identity theft requires a business to have processes in place to not just detect and prevent it but to learn from their experiences and to have protocols in place so that relevant personnel know when to contact senior management, internal security and even when to bring in appropriate law enforcement personnel if and when necessary.

Mitigating identity theft may also mean attempting to contact the person whose identity may have been stolen to notify them that a fraudulent application has been submitted in their name. This allows the potentially affected individual to take their own steps to further mitigate the identity theft risks that they have been exposed to. This can be accomplished by having the potential victim place a fraud alert on their credit files and, if determined that they have actually been a victim of identity theft, to even go so far as to place a security freeze on their account.

It is important to note that while preventing and mitigating identity theft are looked at as two separate duties under the Red Flag provisions of the FACT Act, they are obviously very closely tied to one another. While it may not always be possible to prevent identity theft, mitigating the potential damage is just as important and any Red Flag program should have some steps outlined for personnel to follow to assist in mitigation.

While stopping further misuse of an identity by a fraudster helps the victim, it will also help “stop the bleeding” so to speak, for the institution. Mitigating identity theft allows the business to be more profitable by limiting the amount of fraud losses experienced by a business. However, the exact method and process used to mitigate identity theft will again vary from business to business and institution to institution.

STEP 7
REPEAT PROCESS
ALL OVER AGAIN
(“PERIODICALLY”)

The most important thing to recognize about developing a written Red Flag program is that the process will never actually be finished. Fraud and identity theft is an ever evolving game of cat and mouse. New scams, methods, and schemes are constantly being tried and refined by those determined to commit fraud. Identity theft and fraud are constantly evolving and what was a threat a year or two ago may no longer be a method used by fraudsters today. New methods of committing fraud, whether they be low tech scams involving the use of “social engineering” or high tech methods using new technologies (or exploiting weaknesses in old technology) are constantly popping up. It is a business’s/institution’s duty to stay current on these evolving trends and to update their Red Flag programs accordingly.

Further, a business or institution must learn from its own experiences with identity theft and fraud and constantly refine and improve their program so that the program is in a constant state of evolution. How often must an identity theft program be revised? The answer is “periodically”.

What does periodically mean though? Every six months? Every year? Every five years? This is not exactly clear. However, it would be safe to say that the program should at least be reviewed on an annual or semi-annual basis. Processes should be implemented so that new experiences with identity theft can be regularly integrated into the program. This constant evolution and revision on a “periodic” basis will ensure that Red Flag programs are meaningful and that such programs actually effectively reduce the incidences of identity theft.

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.