

# Designing an Identity Theft Prevention Program



**The Federal Trade Commission has indicated that mortgage brokers are covered by the Red Flags Rule and must design identity theft prevention programs to comply with the law.**

The FTC has published a How-To Guide for Businesses on Red Flags compliance, titled “Fighting Fraud with the Red Flags Rule.” To get started on designing your Identity Theft Prevention Program, read it here:

<http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf>

**The Red Flags Rule requires brokers to implement a *written* Identity Theft Prevention Program.**

This guide helps you write your own Identity Theft Prevention Program – your Program is the central document your business needs for compliance with the Red Flags Rule law.

Included are suggestions to follow and an example policy and procedures template which, when amended, can become the core of a program specific to your mortgage brokerage.

**Designing your Identity Theft Prevention Program requires a four-step process:**

1. **Identify** the “Red Flags” that are relevant to your business
2. Determine how you will **Detect** these “Red Flags”
3. Establish how your program will **Respond** to “Red Flags” and help **Prevent/Mitigate** identity theft
4. Decide how you will **Implement** and **Evaluate** your Program (sign-off, training, update)

Through these four steps, the decisions you make about identity theft and your business will become the fundamentals of your Program.

**Here’s the Key!**

***Compliance also requires that your Identity Theft Prevention Program be written down.***

**The template included below provides you “fill in the blanks” to develop a written program that addresses all the key requirements of the Red Flags Rule.**

Only you can identify the risks and Red Flags relevant to your business and describe your procedures to detect, prevent, and mitigate identity theft – this guide will give you a framework to get started and a process to follow in using the template to create your own written Identity Theft Prevention Program.

## Step 1: Identify the Red Flags that are relevant to your business

“Red Flags” are suspicious patterns or practices, or specific activities that indicate the possibility of identity theft; they are warning signs that a possible *identity* problem is present.

The Red Flags Rule legislation points out four categories of common Red Flags, and lists 26 specific examples (detailed in Supplement A to the Red Flags Rule), several of which likely apply to your business as a mortgage broker:

Category	Specific Example (as written in Red Flags Rule legislation)
Alerts, Notifications and Warnings from a Credit Reporting Company	<ul style="list-style-type: none"><li>▪ A fraud or active duty alert is included with a consumer report</li><li>▪ A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of FACTA</li></ul>
Suspicious Documents	<ul style="list-style-type: none"><li>▪ Documents provided for identification appear to have been altered or forged</li><li>▪ An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.</li></ul>
Suspicious Personal Identifying Information	<ul style="list-style-type: none"><li>▪ 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 for correlation between the SSN range and date of birth.</li><li>▪ 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:<ul style="list-style-type: none"><li>○ The address on an application is fictitious, a mail drop, or prison; or</li><li>○ The phone number is invalid, or is associated with a pager or answering service</li></ul></li></ul>
Unusual Use of, or Suspicious Activity Related to, the Covered Account	<ul style="list-style-type: none"><li>▪ 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.</li></ul>

**Note:** This is only a *partial* list of the 26 specific examples of “Red Flags” listed in Supplement A to the Red Flags Rule – to view all 26, reference the original text here:

[Click to view FACTA 26 Suggested Red Flags \(pdf\)](#)

As a mortgage broker, you need to consider all stages of your involvement with a borrower’s identity information: from taking the initial loan application and collecting documentation, to closing and storing the borrower’s loan file.

If you have a system that supports any kind of online loan tracking for your borrowers, you should also consider how your clients/employees access that information and what Red Flags might warn you that the wrong person was attempting to gain access. For instance, many companies consider a series of failed attempts to login to a password-protected website a Red Flag indicating someone may be trying to break into an account.

### ***Informative Research***

13030 Euclid Street Garden Grove, CA 92843 T: 714.638.2855 • F: 714.636.2510 [info@informativeresearch.com](mailto:info@informativeresearch.com) • [www.informativeresearch.com](http://www.informativeresearch.com)

*This material has been prepared for educational and informational purposes only and should not be construed as an offering of either legal advice or a legal opinion on any specific matter. It should not be used to replace the advice of your own legal counsel. It is expressly written to frame the primary content elements needed for a Red Flags Identity Theft Program and written also with the presumption that the user entity has committed to including Informative Research’s Red Flags Risk Platform (RFRP) as a critical core element of that program. RFRP has its own express use limits, representations, and warranties stated at the top of each Red Flags Addendum that are also relevant.*

In the Program Template section of this guide, you can fill in the Identity Theft Red Flags you identify when you think through your relationship and work with your borrowers. To get you started, some widely applicable Red Flags have already been listed for you.

As an Informative Research customer receiving the Red Flags Risk Platform, you can identify 9 of the 26 FACTA ‘Suggested Alerts’ (and 8 of the specific sub-examples [i.e. 4 a. and 4 b., 10 a. and 10 b., etc.]) from credit report data and bureau ‘fraud alerts’ – the Red Flags detected by the Platform are very likely applicable to your business as a mortgage broker.

## **Step 2: Determine how you will detect Red Flags**

Once you’ve identified the Red Flags that might surface in your business, your next step is to make sure that you and/or your staff will notice when one of them pops up. Because most of your identity theft risk as a mortgage broker probably pertains to the application process, pay special attention to how you will make sure you and your staff are trained in recognizing Red Flags when they occur. Everyone in your office will need to learn to think a little bit like a detective: on the lookout for suspicious documents, credit report alerts, concerns voiced by borrowers, etc.

In the Program Template section of this guide, fill in the measures you will take to ensure that your business recognizes Red Flags when they occur. Some common approaches have been pre-entered for you to keep, remove or edit as applicable to your business practices. Because you’re using IR’s Red Flags Risk Platform, detection of alerts based on the borrower’s credit and ‘fraud alert’ data is easy for you to document – the Platform automatically lists ‘fraud alerts’ that fire on the borrower’s identify information, and each ‘fraud alert’ includes information on which specific Red Flags from the list of FACTA 26 ‘Suggested Alerts’ apply for that alert.

## **Step 3: Establish how your program will respond to “Red Flags” and help prevent/mitigate ID theft**

This is the heart of your Identity Theft Prevention Program. If a Red Flag is detected and suggests something suspicious might be going on, what will you do about it to protect the consumer?

The Red Flags Rule requires you to respond appropriately to any Red Flag. What is appropriate depends on the level of risk involved. An appropriate response to a credit report alert might simply be to take an extra step in loan processing to further verify your borrower’s identity, or to call the consumer at the telephone number as directed in the alert. But if you receive 20 alerts in one day telling you that 20 of your borrowers provided Social Security numbers belonging to deceased persons, that might make you suspect that criminals are trying to use your business in a larger fraud scheme—in which case, the appropriate response would be to notify law enforcement.

Most of the time, though, a Red Flag will probably be just a warning or trigger to look a little closer at your borrower and his or her application, just to be sure that nothing is wrong. More often than not, following your procedures to mitigate and prevent identity theft will simply result in your loan going forward with better documentation. If the steps you take really do reveal a fraud, such as an applicant using someone else’s identity, catching that fraud before you submit the loan for funding will make a *big* difference for both you and for your lending partners.

Because most brokers are involved in the process of opening an account but not in servicing it over time, most of your responses to Red Flags will probably be focused on ensuring that Red Flags are resolved during the application process such that you are confident no identity theft is involved, or stopping the loan process if suspicions remain.

The Red Flags Risk Platform you receive with each IR credit report will provide you and your staff with “suggested actions” to assist you in resolving any credit data alerts that are triggered, offering a high level of

confidence that your responses to these specific Red Flags will be appropriate in the specialized context of your business as a mortgage broker.

In the Program Template, you can add all of the procedures your business will take to respond to Red Flags when they arise. Your descriptions should be fairly specific, unless they cross-reference written procedures you have already created separately for your employees.

#### **Step 4: Decide how you will implement and assess your Program (sign-off, training, update)**

In order to be effective, your Identity Theft Prevention Program must be familiar to everyone working in your company. Although many of the procedures you'll be using to detect and prevent identity theft may already be common practice in your office, you'll need to be confident your staff understands all the procedures and the contexts in which they should be applied.

Risks change over time, so your Identity Theft Prevention Program needs to change too. The Red Flags Rule sets out specific steps you need to take to ensure that your Program is officially adopted by your company and then formally updated as necessary to keep pace with changes in your company, your business procedures, and the risk environment.

Your written Program should describe both how you will train your employees about Red Flags and how you will keep your Program current.

See the Program Template for ideas on how to approach this.

If you use third party service providers to assist you in handling your covered accounts (most likely your borrowers' loan applications), your written Program must also describe how you will ensure that those service providers are conscious of the risks of identity theft and the measures they take to detect Red Flags and prevent identity theft.

When you finish designing your Program, take the written document to your Board of Directors for approval, or to a senior officer of your company if there is no Board.

In the Program Template, there is a space for you to document the Board's approval.

You should plan on reviewing your Program after a certain amount of time has passed, or after a fraud is detected, a new Red Flag is foreseen, or a major change to the way your borrower's identity information is handled. The Red Flags Rule is specific in calling for Programs to be periodically updated as risks and fraudsters change with your business. See the 'Program Updates' section of the Program Template.

#### **Written ID Theft Prevention Program Template:**

[Click to access the Program template in Microsoft Word format.](#)

---

#### ***Informative Research***

13030 Euclid Street Garden Grove, CA 92843 T: 714.638.2855 • F: 714.636.2510 [info@informativeresearch.com](mailto:info@informativeresearch.com) • [www.informativeresearch.com](http://www.informativeresearch.com)

*This material has been prepared for educational and informational purposes only and should not be construed as an offering of either legal advice or a legal opinion on any specific matter. It should not be used to replace the advice of your own legal counsel. It is expressly written to frame the primary content elements needed for a Red Flags Identity Theft Program and written also with the presumption that the user entity has committed to including Informative Research's Red Flags Risk Platform (RFRP) as a critical core element of that program. RFRP has its own express use limits, representations, and warranties stated at the top of each Red Flags Addendum that are also relevant.*