Complying with the Red Flags Rule:
A Do-It-Yourself Prevention Program for Businesses and Organizations at Low Risk for Identity Theft

The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program to detect the warning signs – or "red flags" – of identity theft in their day-to-day operations. By focusing on red flags now, you'll be better able to spot an imposter using someone else's identity to get products or services from you. As a practical matter, the Rule applies to you if you provide products or services and bill customers later. To find out if the Red Flags Rule applies to your business, read ***Fighting Fraud with the Red Flags Rule: A How-To Guide for Business***, a booklet published by the Federal Trade Commission (FTC).

The FTC, the federal agency that enforces a number of consumer protection laws, has designed this compliance template to help businesses and organizations at low risk for identity theft design their own Identity Theft Prevention Program. It has two parts: **Part A** to help you determine whether your business or organization is at low risk, and **Part B** to help you design your written Identity Theft Prevention Program if your business is in the low risk category.

PART A: Is your business or organization at low risk for identity theft?

How can you tell if your business is at low risk for identity theft? Conduct an assessment. Although you have to consider the unique characteristics of your business, here are some factors to help you decide your risk level.

- **Do you know your clients personally?** Perhaps you're a doctor or a lawyer on Main Street and are familiar with everyone who walks into your office. It's unlikely that an identity thief can defraud you by impersonating someone you already know. That would place your business at low risk for identity theft.

- **Do you usually provide your services at your customers' homes?** To avoid getting caught, identity thieves tend to move around a lot. They generally don't want people to know where they live. If you regularly provide services at your customers' homes, your business may be at low risk for identity theft.

- **Have you ever experienced an incident of identity theft?** You've been in business for some time now, and no one has complained that someone stole his identity and used it to get products or services at your business. That might suggest your business is at low risk for identity theft.

- **Are you in a business where identity theft is uncommon?** If there are no reports in the news and no talk among people in your line of work about identity theft, your industry may not now be the target of identity thieves, and your organization may be at low risk for identity theft.

I've conducted an assessment of Cranbrook Loans Group, Inc

name of your business or organization

Here are the reasons we are at low risk for identity theft:

Our firm's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. We will do this by developing and implementing this written ITPP, which is appropriate to our size and complexity, as well as the nature and scope of our activities. This ITPP addresses 1) identifying relevant identity theft Red Flags for our firm, 2) detecting those Red Flags, 3) responding appropriately to any that are detected to prevent and mitigate identity theft, and 4) updating our ITPP periodically to reflect changes in risks.

Our identity theft policies, procedures and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our business.

This space holds up to 1550 characters. Use an additional sheet if necessary.

PART B: Designing an Identity Theft Prevention Program for Businesses or Organizations at Low Risk

Designing a program involves four basic steps:

STEP 1: Identifying relevant red flags

STEP 2: Detecting red flags

STEP 3: Responding to red flags

STEP 4: Administering your Program

STEP 1: Identifying relevant red flags

The first step is to identify the relevant red flags you might come across that signal that people trying to get products or services from you aren't who they claim to be. Read the FTC's free booklet ***Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*** (pages 19-21) for examples. For instance, if you check photo IDs, a classic red flag of identity theft is an inconsistency between the person's appearance and the information on the photo ID. If you know all your customers personally, it's probably not necessary to ask for a photo ID, and this red flag wouldn't be appropriate. Sometimes, the only red flag may be a notice from another source that an identity theft has occurred. Since that red flag applies to everyone, it's included here.

Here are the red flags we have identified:

1. Notice from a customer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently.
2. Suspicious Documents
3. Suspicious Account Activity
4. suspicious personal identifying information

Each space holds up to 210 characters. Use an additional sheet if necessary.

STEP 2: Detecting red flags

The second step is to explain how your business or organization will detect the red flags you've identified. For example, perhaps in Step 1 you identified false IDs as a red flag. To detect a false ID, you might consider training your staff to look carefully at the ID to see if the person's appearance is consistent. What if somebody notifies you that an account has been opened or used fraudulently? To make sure those notices don't fall through the cracks, you may decide to require employees to log that kind of notice in a central place or to tell a staff member responsible for responding to red flags.

Here's how we'll detect the red flags we have identified:

1. Authenticating Customers who apply
2. Monitoring applications
3. Verifying the validity of each person we speak with
4. ensuring the applicant and their spouse provide direct information.

Each space holds up to 210 characters. Use an additional sheet if necessary.

STEP 3: Responding to red flags

The third step is to decide how you'll respond to any red flags that materialize. For example, say you've identified the risk of false IDs as a warning sign of identity theft, and you've noted that you will train your staff to look for inconsistencies in identification. Your employee has checked the photo ID and detected an inconsistency. What's the next step? Perhaps it's asking for another form of identification – or maybe not providing any products or services until the inconsistency has been resolved. Or imagine you're trying to collect on an unpaid bill, and the person you contact tells you his identity was stolen and he didn't run up that bill. Although it will depend on the circumstances, consider how you might respond. For example, you could ask for proof that an identity theft claim has been filed.

Here's how we'll respond to the red flags we have identified:

1. Get more information from customer
2. Document the information, and dates
3. Report to Federal and state authorities
4. If organized then report to FBI or secret service or Postal Inspector if applicable.

Each space holds up to 210 characters. Use an additional sheet if necessary.

STEP 4: Administering your Program

The last step is documenting how you'll administer your Program. Here's what's involved:

- **Get the approval of your Board of Directors, a committee of your Board, or a senior manager.**

Our Program has been approved by:

Michael Ayoub

name

- **Designate a senior employee to administer your Program.**

The person who will administer our Program is:

Michael Ayoub

name

- **Describe how you'll train your staff.** List the categories of employees who will be trained to detect red flags – for example, your reception staff or the people who handle your accounts receivable – and how they'll get that training – say, during an orientation for new employees or an annual update.

Here are the categories of employees we'll train and how we'll provide training:

Category of employee	How we provide training
All Employees	In Person Training

Use an additional sheet if necessary.

- **Describe how you'll supervise your service providers.** Do you use service providers who might detect any of the red flags you've identified? For example, do you hire a company to handle your invoicing or use a collection agency to collect overdue bills? Talk to them to see that they're following your Program or have their own that complies with the Red Flags Rule.

☒ We don't use service providers in connection with accounts covered by the Red Flags Rule.

☐ We use service providers in connection with accounts covered by the Red Flags Rule.

Here are the service providers we'll contact about complying with the Red Flags Rule:

1.

2.

3.

4.

Each space holds up to 210 characters. Use an additional sheet if necessary.

- **Describe how you'll update your Program.** Identity theft risks can change fast, so it's important to reassess your Program periodically. If your business experiences identity theft, if any factors change that contributed to your original assessment of low risk, or if you change your business model with respect to your accounts or your corporate structure, you will need to re-evaluate and modify your Program.

Here's how we'll keep our Program current:

1. Annual Review
2. Update Training
3. Periodic Testing
4. Integrate with processing

Each space holds up to 210 characters. Use an additional sheet if necessary.

Questions about complying with the Red Flags Rule?

Visit **ftc.gov/redflagsrule** or email **RedFlags@ftc.gov**.

Print a copy for your records.