Sample Red Flags Identity Theft Policy for Fintech Program Managers

The following is not legal advice and should only be used as starting precedents and operational best practices. Each product and company is unique, and you should consult with an experienced lawyer licensed in the relevant jurisdiction(s) to tailor the sample as needed.

Lithic does not assume responsibility for the contents of, or the consequence of using, any version of these documents or any other document found on our website. Lithic's legal team knows many fintech lawyers and we're happy to point Lithic customers to recommendations.

1. To help you fill out this sample policy, we've added some footnotes with considerations and yellow-highlighted brackets and prompts for you to fill in information. We've additionally orange-highlighted particular sections that depend on particular companies' practices.
2. All highlighted brackets should be accurately completed and all footnotes should be deleted before the sample is finalized. Consider searching for "[" and "]" to make sure you don't miss any.
3. The terms should be reviewed generally to ensure they accurately reflect your operations and practices (without removing any legally required sections).
4. Finally, delete this instructions page.

Other card program-related legal forms can be found in our documentation.

If you need more suggestions on how to build your compliance program, check out Lithic's Fintech Layer Cake podcast, available on major podcast and video streaming platforms.

* * * *

Table of Contents[1]

[1] When the policy is final or near-final, update the table of contents in case any sections were added or removed, and to ensure correct page numbers.

1. Summary and Overview

It is the policy of [[Company Legal Name]], ("[[Company]]" or "Company") to fully comply with and support its Bank Partners in their compliance with Identity Theft prevention program requirements under the Fair and Accurate Credit Transactions Act ("FACTA") and Red Flags Rule promulgated by the Federal Trade Commission ("FTC"). As part of this effort, the Company has developed and maintains an Identity Theft prevention program ("Program").

[[Company]] is not a bank, a bank holding company, or a subsidiary of a bank or a bank holding company. However, [[Company]] partners with banks (each, a "Bank Partner") to provide services to its customers that are within the scope of Bank Partners' Identity Theft Red Flags obligations. Accordingly, [[Company]] takes its role in ensuring Identity Theft Red Flags compliance very seriously, and strives to promote compliance throughout its organization..

The Company's [[Board of Directors]][2] has adopted this Identity Theft Red Flags Policy ("Policy") as part of its compliance management system. The [[Compliance Officer]][3] has been designated as the person responsible for the Policy and the Company's Program.

For purposes of this Policy:

- "Covered Account" means an account, [[including an extension of credit]],[4] that the Company or its Bank Partner offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the Bank Partner from Identity Theft.

- "Identifying Information" includes any name or number that may be used, alone or with other information, to identify a specific person, including: (i) a name, Social Security number, date of birth, government-issued identification number, alien registration number, government passport number, employer, or taxpayer identification number; (ii) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (iii) unique electronic identification number, address, or routing code; or (iv) telecommunications identifying information or access device.

- "Identity Theft" means a fraud committed or attempted using Identifying Information of another person without authorization.

- "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

- "Senior Management" means the Company's executives and senior managers.[5]

[2] You may consider having the policy adopted by your management team, if your company is small and/or your board is not generally involved in oversight of your programs. If you go that route, you'll want to confirm this is OK with your bank partner.
[3] We've put this in brackets in case you don't have a compliance officer yet. This might be a business-focused co-founder if you're a small team, or a compliance manager if you've hit product-market-fit but aren't ready for a full compliance officer yet. Given Red Flags involves fraud and risk, you also might have this roll up to your fraud or risk lead.
[4] Remove if your bank partners require you to have a red flags policy for non-credit products.
[5] You may wish to tailor further depending on the scale and size of your company.

2. Scope

This Policy applies to all of the Company's administrative, technical, and physical policies, procedures, and practices concerning the opening and maintenance of Covered Accounts that relate to the prevention, detection, and mitigation of Identity Theft.

This Policy applies to the Company's employees, vendors, and any other individual whose duties in any way involve activities related to Covered Accounts. Such individuals are expected to cooperate fully with any Red Flags assessment being conducted as part of the Program in departments or divisions for which they are accountable. Employees are further expected to work with the Company's [[Compliance Team]] and [[Compliance Officer]][6] to develop any required Identity Theft prevention, detection, or mitigation plans.

3. Roles and Responsibilities

3.1 Company Board of Directors[7]

The Company's Board oversees and is ultimately responsible for ensuring that the Company adheres to all applicable laws and company policies. The Board (or a designated Committee of the Board) is responsible for reviewing and approving this Policy and any changes or modifications to the Policy as they occur. The Board may designate its ability to approve changes to the Policy to an executive of the Company. The Board also maintains oversight of compliance with Policy and any significant risks that Senior Management identifies.[8]

3.2 [[Compliance Officer]][9]

The [[Compliance Officer]] is responsible for evaluating and updating the Policy to reflect any changes to (i) operations regarding the maintenance and opening of Covered Accounts, (ii) Company employees whose duties in any way involve Covered Accounts, or (iii) applicable laws, as described in Section 8 (Laws, Rules, Regulations and Other Sources) of this Policy. The [[Compliance Officer]] reviews the Policy on a periodic basis and when any such changes are made. The [[Compliance Officer]]'s review includes consideration of feedback on the effectiveness of the Policy and any input from the Bank Partner.

3.3 Customer Service

Individuals engaging in customer service activities are in a unique position to help identify Identity Theft, and are directed to follow specific procedures to identify Red Flags that may surface during the customer service and account opening processes.

---

[6] Given identity theft falls more in the realm of risk and fraud issues, you may wish to have this reference your internal fraud or risk departments and leads.
[7] You might edit this so oversight falls to your Senior Management team. If so, see the next footnote.
[8] Senior Management oversees and is ultimately responsible for ensuring that the Company adheres to all applicable laws and company policies. Senior Management is responsible for ratifying any changes to this Policy on a periodic basis. Senior Management also maintains oversight of compliance with Policy and any significant risks that the Compliance Officer identifies.
[9] Reminder to update the title in this section in case you do not have a compliance officer.

3.4 Risk and Compliance[10]

The Company's Risk and Compliance teams are in a unique position to help identify Identity Theft, and are directed to follow specific procedures to identify Red Flags that may surface during their review of accounts and transactions.

3.5 Legal[11]

The Company's legal team ensures the Company's compliance with applicable Identity Theft laws, which are described at the end of this Policy. Legal team members advise on requirements of Identity Theft laws applicable to the Company's programs and services. Where appropriate, the Company also engages outside counsel to advise on Identity Theft matters.

3.6 Periodic Review

The Company shall identify and appoint appropriately skilled and knowledgeable persons[12] to be responsible for conducting periodic control testing and review of the policy's effectiveness.

4. Identity Theft Prevention Program

FACTA requires financial institutions such as the Company's Bank Partners to develop and implement a written Program to detect, prevent, and mitigate Identity Theft in connection with the opening and maintenance of Covered Accounts.[13] In particular, banks must develop reasonable policies and procedures to identify, detect, and respond to appropriate Red Flags. While the Company makes every effort to maintain the confidentiality of its customers' nonpublic information, this Policy ensures that the Program enables its Bank Partners to comply with the Red Flags Rule's requirement to protect customer information from Identity Theft.

4.1 Basic Components of the Program

With respect to activities involving Covered Accounts, the Company complies with all requirements as set forth by the Red Flags Rule, including, but not limited to, implementing the following Program components:

- Risk Assessment and Mitigation;

[10] If you've achieved product-market fit, you are likely building dedicated risk and compliance teams. If not, you'll want to delete or tailor this section.
[11] If you do not yet have an in-house legal team, you might consider this alternative language: The Company's outside counsel and other advisors advise on the applicable Identity Theft laws, which are described at the end of this Policy. The Compliance Officer works with these advisors to ensure the Company has an up-to-date understanding of legal requirements.
[12] Internal compliance, legal or risk professionals may be able to help conduct this review. Lithic can also recommend consultants to assist with any periodic reviews you or your bank partners would like to conduct.
[13] See the FTC's definition of "covered account" at 16 C.F.R. pt. 681.1(b)(3) ("[a]ny other [non-consumer] account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks").

- Identifying Red Flags;
- Detecting and Responding to Red Flags;
- Compliance Monitoring; and
- Training.

4.2 Risk Assessment and Identifying Red Flags

To identify (i) Covered Accounts covered by the FTC's Red Flags Rule and (ii) Red Flags, the Company performs a risk assessment that is presented to the Company's Board and Senior Management[14] and incorporates relevant Red Flags from other sources.

Risk Assessment. The Company conducts a periodic risk assessment to identify which accounts are Covered Accounts for purposes of the Program. In conducting this risk assessment, the Company may consider the following factors:

- The risks inherent in the Bank Partners' products or the Company's maintenance of accounts;
- The methods it provides to persons who open an account or apply for a Bank Partner's product;
- The methods it provides to persons to access an account or a Bank Partner's product; and
- The Company and the Bank Partner's previous experiences with Identity Theft.

Sources of Red Flags. In identifying Red Flags, the Company incorporates Red Flags from sources such as:

- Incidents of Identity Theft that the Bank Partner or the Company has experienced;
- Methods of Identity Theft that the Bank Partner or the Company have identified that reflect changes in Identity Theft risks; and
- Applicable supervisory guidance.

Examples of Red Flags. Examples of Red Flags that may be identified and incorporated into the Identity Theft Red Flags Procedures include, but are not limited to, the following:

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;

[14] If your board is not directly involved in day-to-day oversight, you might tailor this so the risk assessment is just presented to senior management or your executives.

- The unusual use of, or other suspicious activity related to, a Covered Account; and
- 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.

4.3 Detecting Red Flags

The Company implements a number of processes to detect Red Flags, as detailed in the Identity Theft Red Flags Procedures. These may include, but are not limited to:

- Following all Know Your Customer Policies, as detailed [[in the Anti-Money Laundering (AML) and Sanctions (OFAC) Program]][15];
- Monitoring the Covered Account for a material change in the customer's use of the Services;
- Making efforts to confirm suspicious documents; and
- Making efforts to confirm new documents that are inconsistent with publicly available (or otherwise externally sourced) documents or documents that are already on file.

4.4 Responding to Red Flags

The Program provides for appropriate responses to the Red Flags that are commensurate with the degree of risk posed. In determining an appropriate response, the Company considers aggravating factors that may heighten the risk of Identity Theft. Appropriate responses may include the following:

- Monitoring a Covered Account for evidence of Identity Theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a Covered Account;
- Reopening a Covered Account with a new account number;
- Not opening a new Covered Account;
- Closing an existing Covered Account;
- Not attempting to collect on a Covered Account;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

[15] Tailor this reference to the title of your AML and Sanctions policy.

4.5 Program Monitoring

The [[Compliance Officer]] shall periodically determine whether the Program requires modification. As part of this determination, consideration should be given to changes in the following activities or processes:

- The Company or the Bank Partner's previous experiences with Identity Theft;
- Changes in methods of Identity Theft;
- Changes in methods to detect, prevent, and mitigate Identity Theft;
- Changes in the types of accounts that the Bank Partner or the Company offers or maintains; and
- Changes in the business arrangements of the Bank Partner or the Company, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

The [[Compliance Officer]] gives the Company's Senior Management a status report on the overall status of initiatives related to Red Flags, regulatory developments and emerging issues, and critical areas of risk at least annually. Any recommended changes to the Program, and the reasons and plans for making such changes are documented and presented to Senior Management.

4.6 Training

Company employees whose duties in any way involve Covered Accounts receive Identity Theft Red Flags training at least annually. In addition to annual training, such individuals receive appropriate retraining upon any changes to the Program, the Procedures, or any applicable Identity Theft laws and regulations described at the end of this Policy. New employees of the Company whose duties in any way involve Covered Accounts will receive Identity Theft Red Flags training during onboarding. The Company ensures that vendors whose services involve Covered Activities have received appropriate Identity Theft Red Flags training.

5. Complaints

Complaints raising Identify Theft issues received through the Company's support channels are routed through customer service channels to the business team for resolution, and any complaints raising compliance issues with respect to Identity Theft laws are raised with the [[Compliance Officer]]. The Company ensures that user-facing vendors have appropriate complaint resolution processes in place.

6. Record Retention and Recordkeeping

The Company maintains records as required by applicable financial services laws, as detailed in each applicable policy.[16]

[16] This reference is meant to tie in specific financial services laws with their own recordkeeping requirements, such as AML and fair lending laws. You can adapt it as needed.

7. Governance

The Company's [[Board of Directors]][17] must approve the initial Program as written in this Policy and the Identity Theft Red Flag Procedures. Thereafter, the Program is a dynamic program that is updated as appropriate, and any updates to the Program or this Policy are approved by the [[Company's Board of Directors]][18]. The [[Compliance Officer]] is involved in the oversight, development, implementation, and administration of the Program.

Changes to the Identity Theft Red Flag Procedures are reviewed and approved in advance of implementation by the [[Compliance Officer]]. In addition, any significant procedural changes are communicated to relevant staff by the [[Compliance Officer]], executive management, or line managers through an appropriate email or training.

8. Laws, Rules, Regulations and Other Sources

This section provides a list of those laws, rules, regulations, guidelines, and other sources of legal guidance that [[Company]] has determined are most relevant to its products, services, and activities. This list is not exhaustive and is subject to periodic review and change, as appropriate.

- FACTA: FACTA, amending the Fair Credit Reporting Act, is codified at 15 U.S.C. §§ 1681 *et seq.*
- FTC Red Flags Rule: The FTC's Red Flags Rule is codified at 16 C.F.R. pts. 681.1 *et seq*

9. Approval, Review and Version History

Version	Changes By	Revision Notations	Date Reviewed
1		Policy drafted; effective date	

[17] If applicable, update references in this section to senior management or executives as necessary to make consistent with the top of this policy.
[18] See note above.