HOOSIER SOCIAL IMPACT FUND INC.
IDENTITY THEFT PREVENTION PROGRAM

Adopted July 31, 2014

I. Purpose of Policy

Hoosier Social Impact Fund Inc. (HSIF) developed this policy to protect its customers and to meet the standards set forth in the Red Flags Rule created by the Federal Trade Commission (FTC) under the Fair and Accurate Credit Transactions Act of 2003 (FACT Act). The Rule requires certain firms to create a written program to identify, detect, and respond to "red flags" that may indicate "identity theft" (i.e., a fraud committed or attempted using another's identifying information without authority).

HSIF's policy is to protect our customers and their accounts from identity theft and to comply with the FTC's Red Flags Rule. HSIF does this by implementing this Identity Theft Prevention Program, which is appropriate to its size, complexity, and the nature and scope of its activities. This program addresses (1) identifying relevant identity theft Red Flags for HSIF; (2) detecting those Red Flags; (3) responding appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and (4) periodically updating its program to reflect changes in risks. HSIF will periodically review and update its identity theft policies, procedures, and internal controls to ensure they account for changes in the law and its business.

II. Designated Identity Theft Officer and Program Administration

HSIF's Vice President (VP) of Communications is the designated identity theft officer and is responsible for the development, implementation, administration, and oversight of HSIF's Identity Theft Prevention Program. The VP of Communications will (1) give HSIF members a copy of this program (and any updated version of this program) to read and keep; (2) train HSIF members in the implementation and administration of this program (and any changes in this program) as appropriate for their duties; (3) ensure new HSIF members do not have any interaction with HSIF's customers and are not given access to customer information until they have been trained under this program; and (4) provide appropriate oversight and training on this program for HSIF's third-party vendors.

III. Relationship to Other HSIF Programs

HSIF has reviewed other policies, procedures, and plans regarding the protection of customer information and privacy, and has modified them and this program to minimize any inconsistencies and duplicative efforts.

IV. Identifying Relevant Red Flags

HSIF considered Red Flags from the following categories as they fit HSIF's operations: (1) alerts, notifications, or warnings from a credit reporting agency; (2) suspicious documents; (3) suspicious personal identifying information; (4) suspicious account activity; and (5) notices from other sources. HSIF understands some of these categories and examples may not be relevant to HSIF or may be relevant only when combined or considered with other ID theft indicators. HSIF also understands that the examples are not exhaustive or mandatory, but are a way to help HSIF think about relevant red flags in its business. Based on its review of the risk factors, sources, and FTC examples of red flags, HSIF identified the Red Flags contained in the table below.

To identify relevant ID theft Red Flags, HSIF assessed these risk factors: (1) the types of accounts it offers; (2) the methods HSIF uses to open or access accounts; and (3) existing experience with and knowledge of identity theft. HSIF also considered the sources of Red Flags, including reported identity theft incidents, changing identity theft techniques HSIF thinks likely, and applicable supervisory guidance.

The following factors indicate that a low risk of identity theft applies to HSIF:

- HSIF is in a type of business where identity theft appears to be rare. It has not experienced any incidents of identity theft, and is not aware of reports of identity theft in this field from the news, the trade press, or similar firms.
- HSIF staff members have personal knowledge and familiarity with each customer in its small group of clients, with whom they work closely.
- HSIF provides services in face-to-face settings where HSIF has already verified the customer's identity.

V. Detecting Red Flags

HSIF reviewed its accounts, how it opens and maintains them, and how it may detect Red Flags. HSIF's detection of Red Flags is based on its methods of getting and verifying applicant information, authenticating customers who access accounts, and monitoring transactions and address change requests. To open accounts, it can include obtaining identifying information and verifying the identity of the person opening the account. For existing accounts, it can include authenticating customers, monitoring transactions, and verifying the validity of address change requests. Based on its review, HSIF created the table below indicating how it will detect each identified Red Flag.

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from Credit Reporting Agency	
1. A fraud alert is included on a credit report or from another source.	Verify that any fraud alert covers an applicant or customer and review the allegations in the alert.
2. HSIF requests a credit report, reference, or other check and receives a credit freeze notice.	Verify that the freeze covers an applicant or customer and review the freeze.
3. A notice of address or other discrepancy is provided by a reporting agency.	Verify notice covers an applicant or customer, review discrepancy, and determine next steps to take.
4. A credit report or other source shows a pattern inconsistent with a person's history (e.g., big increase in credit use or inquiries, high number of new credit accounts; account closed for abuse).	Verify that credit report covers an applicant or customer, and review the degree of inconsistency with prior history.
Category: Suspicious Documents	
5. ID presented looks altered or forged.	Scrutinize ID presented to make sure it is not altered or forged, report any instances to the VP of Communications.

6. The ID presenter does not look like the ID's photograph or physical description.	Ensure that ID photo and physical description match presenter, refuse to open an account if they do not match, and report instances to the VP of Communications.
7. Information on the ID differs from what the ID presenter is saying.	Ensure that the ID and the statements of the person presenting it are consistent, and report any instances to the VP of Communications.
8. ID information doesn't match information on file (e.g., original application, signature card, check).	Ensure that ID information is consistent with information on file for an account.
9. The application looks like it has been altered, forged, or torn and reassembled.	Scrutinize each application to make sure it is not altered, forged, or torn and reassembled, report any instances to the VP of Communications.
Category: Suspicious Personal Identifying Information	
10. Inconsistencies between information presented and information known about presenter or discoverable through readily available sources (e.g., address does not match credit report, SSN is not issued or is listed on SSA Death Master File).	Check personal identifying information to ensure that SSN given has been issued and not listed on the SSA's Master Death File, check credit report to see if addresses on application and report match, and report inconsistencies to the VP of Communications.
11. Inconsistencies exist in information provided by the customer (e.g., birth date does not fall within the number range on the SSA's issuance tables).	Check personal identifying information for internal consistency (e.g., compare birth date and number range for SSN on SSA issuance tables).
12. Personal identifying information presented has been used on an account known to be fraudulent.	Compare information presented by customer with addresses and phone numbers on accounts or applications found or reported to be fraudulent.
13. Personal identifying information presented suggests fraud (e.g., an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service).	Validate information presented when opening an account by looking up an address on the Internet to ensure it is real and not for a mail drop or a prison, and call phone numbers to ensure validity.
14. The SSN presented was used by others or to open other accounts.	Compare customer SSN to see if it was given by others or used on other accounts.
15. The listed address or telephone number has been used by other people or for other accounts.	Compare address and telephone number to existing information to see if they were used by other applicants or customers or for other accounts.
16. A person who omits required information on an application or other form fails to provide it when asked to do so.	Track when applicants or customers fail to respond to information requests, determine why they failed to respond, and consider when deciding whether to maintain or open an account.
17. Inconsistencies exist between information that is presented and information already on file.	Compare information presented with information on file, attempt to resolve inconsistencies, report unresolved inconsistencies to the VP of Communications to investigate.

18. Applicant or person seeking account access cannot provide authenticating information beyond what would be found in a wallet or credit report, or cannot answer a challenge question.	Authenticate identity for customers by asking challenge questions prearranged with the customer, and for applicants or customers by asking questions that require information not readily available from a wallet or a credit report.
Category: Suspicious Account Activity	
19. Soon after HSIF gets a change of address request for an account, it is asked to add additional users or access means.	Verify request to change address by sending a notice to new and old addresses so customer can learn of unauthorized changes and notify HSIF.
20. A new account exhibits fraud patterns (e.g., first payment is not made or is the only payment made, use of credit for cash advances and securities easily converted into cash).	Review account activity to ensure that payments are made, and that credit is not primarily used cash advances or securities easily converted to cash.
21. An account shows a new pattern of activity, such as nonpayment inconsistent with prior history, or material increase in credit use or spending).	Check accounts on at least a monthly basis for suspicious activity (e.g., non-payment, big increases in credit use or spending).
22. An account that is inactive for a long time is suddenly used again.	Check accounts on at least a monthly basis to see if inactive accounts become active.
23. Mail to a customer is returned as undeliverable, but the account is active.	Note any returned mail for an account and immediately check the account's activity.
24. HSIF learns that a customer is not getting his or her account statements.	Record and investigate any report that a customer is not receiving statements.
25. HSIF is notified that there are unauthorized transactions for an account.	Verify if the notification is legitimate and involves an account, then investigate.
Category: Notice From Other Sources	
26. A customer, victim, or law enforcement reports that an account was opened or used fraudulently.	Verify that the notification is legitimate and involves an account, and then investigate.
27. HSIF learns that unauthorized access to a customer's personal information took place or is more likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	Contact the customer to learn the details of the unauthorized access to determine next steps.

VI. Preventing and Mitigating Identity Theft

HSIF has reviewed its accounts, its procedures for opening and accessing them, and existing and foreseeable methods of identity theft. Based on this and a review of resources regarding identity theft prevention (including FTC rules and suggested actions), HSIF has developed procedures to respond to identity theft Red Flags.

A. Procedures to Prevent and Mitigate Identity Theft

When HSIF detects a Red Flag, it will take the steps outlined below that are appropriate to the type and seriousness of the threat:

1. Applicants

For Red Flags raised by someone applying for an account:

1. Review the application. HSIF will review the information collected from the applicant (e.g., name, date of birth, address, Social Security Number or EIN).

2. Get government identification. If the applicant is applying in person, HSIF will also check a current government-issued ID, such as a driver's license or passport.

3. Seek additional verification. If the potential risk of identity theft indicated by the Red Flag is probable or large in impact, HSIF may also verify the person's identity through non-documentary methods, including but not limited to:

a. Contacting the customer;

b. Independently verifying the customer's information by comparing it with information from a credit reporting agency, public database, or other source such as a data broker or third-party service provider;

c. Checking references with other affiliated financial institutions; and/or

d. Obtaining a financial statement.

4. Deny the application. If HSIF finds that the applicant is using an identity other than his or her own, it will deny the application.

5. Report. If HSIF finds that an applicant is using an identity other than his or her own, HSIF will report it to appropriate local and state law enforcement and regulatory authorities, to the FBI or Secret Service if organized or widespread crime is suspected, and to the U.S. Postal Inspector if mail is involved.

6. Notification. If HSIF determines that personally identifiable information has been accessed, HSIF will prepare adequate notices to customers, including but not limited to all notices required by law.

2. Access seekers

For Red Flags raised by someone seeking to access an existing account:

1. Watch. HSIF will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.

2. Check with customer. HSIF will contact the customer, describe what HSIF has found, and verify if there has been an attempt at identify theft.

3. Heightened risk. HSIF will determine if there is a particular reason that makes it easier for an intruder to seek account access (e.g., a customer's lost wallet, mail theft, a data security breach, or the customer giving information to an imposter pretending to represent HSIF or to a fraudulent web site).

4. Check similar accounts. HSIF will review any similar accounts maintained by HSIF to see if there have been attempts to access them without authorization.

5. Collect incident information. For a serious threat of unauthorized account access HSIF may collect (if available):

a. The violator's name and contact information (e.g., telephone number)

b. Dates and times of activity;

c. Details of any transaction or account activity;

d. Accounts affected by the activity, including name and account number, and

e. The applicant's or customer's losses (if any) and whether they will be reimbursed (and by whom).

6. Report. If HSIF finds unauthorized account access, HSIF will report it to appropriate local and state law enforcement; to the FBI or Secret Service if organized or widespread crime is suspected; and to the U.S. Postal Inspector if mail is involved.

7. Notification. If HSIF determines personally identifiable information has been accessed that results in a foreseeable risk for identity theft, HSIF will prepare adequate notices to customers, including but not limited to all notices required by law.

8. Review our insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, HSIF will review its insurance policies (if any) to ensure that its response does not limit or eliminate any insurance coverage.

9. Assist the customer. HSIF will work with customers to minimize the impact of identity theft by taking the following actions, as applicable:

a. Offering to change the password or other ways to access the threatened account;

b. Offering to close the account;

c. Offering to reopen the account with a new account number;

d. Not collecting on the account or selling it to a debt collector; and

e. Instructing the customer to go to the FTC Identity Theft Website to learn steps to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue NW, Washington, DC 20580.

VII. Other Service Providers

HSIF may use third-party service providers in connection with its covered accounts. HSIF will have a process to confirm that any service provider that performs activities in connection with our accounts comply with reasonable policies and procedures designed to detect, prevent and mitigate identity theft by contractually requiring them to have policies and procedures to detect and report the Red Flags identified in this policy.

VIII. Internal Compliance Reporting

HSIF staff members who are responsible for developing, implementing and administering its Identity Theft Prevention Program will report at least annually to HSIF officers and Board of Directors on HSIF's compliance with the FTC's Red Flags Rule. The report will address the effectiveness of HSIF's Identity Theft Prevention Program in addressing the risk of identity theft in connection with account openings, existing accounts, service provider arrangements,

significant incidents involving identity theft, and any response and/or recommendations for material changes to the program.

IX. Updates and Annual Review

HSIF will update this plan whenever it has a material change to its operations, structure, business, or location, or when it experiences either a material identity theft from a covered account, or a series of related material identity thefts from one or more covered accounts. HSIF will also follow new methods of identity theft and evaluate the risk they pose for HSIF. In addition, HSIF will review this program annually to modify it for any changes in HSIF's operations, structure, business, or location.

X. Approval

HSIF's Vice President of Communications and designated identity theft officer approved this Identify Theft Prevention Program on July 31, 2014, as reasonably designed to enable HSIF to detect, prevent and mitigate identity theft.