

**Customer Identification Program Procedures**

Effective Date: July 22, 2020

Contents

[1. OVERVIEW 3](#_Toc34731397)

[1.1 Scope 3](#_Toc34731398)

[1.2 Related Documents and governing law 3](#_Toc34731399)

[2. CUSTOMER INFORMATION REQUIRED 3](#_Toc34731400)

[3. IDENTITY VERIFICATION 4](#_Toc34731401)

[4. RECORDKEEPING 5](#_Toc34731402)

[5. COMPARISON WITH GOVERNMENT LISTS 5](#_Toc34731403)

[6. CUSTOMER NOTICE 6](#_Toc34731404)

[7. TESTING PROCEDURES AND CONTROLS 6](#_Toc34731405)

[8. ROLES AND RESPONSIBILITIES 7](#_Toc34731406)

[9. dOCUMENT mANAGEMENT 7](#_Toc34731407)

# OVERVIEW

iCreditWorks’ (alternatively referred to as “iCW” or “Company”) Customer Identification Program (CIP) is a fundamental control in preventing the Company from becoming involved in money laundering, terrorist financing, or sanctions violations. As such, these CIP Procedures describe:

* Identifying information that is obtained from every customer opening a new account
* Technology utilized to verify identifying information provided by a customer in the course of opening an iCW account
* Actions taken by iCW in the event that the Company is unable to form a reasonable belief that it knows the true identity of a customer
* Records created and maintained by iCW with respect to its CIP
* Government lists utilized at onboarding
* Customer notice of iCW’s efforts to collect and maintain records related to the CIP

## Scope

These Procedures govern all aspects of iCW’s CIP, and they are applicable to all personnel at iCW, including both employees and consultants. It is also applicable to all third parties with whom iCW has business arrangements for ongoing operational activities. Third parties include, but are not limited to, dental office partnerships, bank partnerships, and service providers.

## Related Documents and governing law

Policies and Procedures:

* *BSA/AML and OFAC Policy*
* *Compliance Management System Policy*
* *Watchlist Screening Procedures*
* *Data Handling and Retention Policy*

Governing Law:

* 31 CFR § 1020.220

# CUSTOMER INFORMATION REQUIRED

iCW’s CIP is fundamental in preventing the Company from becoming involved in money laundering, terrorist financing, or sanctions violations. In the course of onboarding a customer, iCW collects the following data:

|  |  |
| --- | --- |
| Name | First name |
| Last name |
| Address | Street address |
| City |
| State |
| Zip Code |
| Identification Number | Social Security Number (SSN) |
| Date of Birth | Date of birth |

The Company will never open an account for customers who:

* Are corporations or other entities;
* Give only a Post Office Box as an address;
* Give a foreign address;
* Do not provide each of the required pieces of information described above;

# IDENTITY VERIFICATION

iCW primarily employs non-documentary methodologies for verifying identifying details input by loan applicants, which consists of comparing applicant data with information obtained via a consumer reporting agency (TransUnion).

TransUnion specifically evaluates identity verification risk via analyzing applicant inputs (first name, last name, address, SSN, and date of birth) against multiple data sources and produces an output risk score for each applicant (pass, flag, or fail).

If an applicant’s TransUnion risk output is “pass”, no serious identification red flags were uncovered, and the application will continue along a standard underwriting and processing path.

If an applicant’s risk output is “flag” based on a CIP-relevant datapoint, they will be asked to provide an answer to a knowledge-based authentication (KBA) question and prompted for additional verification documents to remediate the specific flag condition(s). The only instance in which a KBA alone may serve to verify a portion of the applicant’s identity are for instances when the specific flag condition generated is regarding the applicant’s address. All other flag conditions (name, SSN, and DOB) must be remedied with documentary evidence. If the additional verification is not received or does not validate the flag condition, the customer must be declined. The table below lists acceptable documents to remediate specific flag conditions.

|  |  |
| --- | --- |
| **Flag Condition** | **Acceptable Remediation Documents** |
| First and/or Last Name | * Unexpired driver’s license * Unexpired military ID * Unexpired passport * Unexpired state ID * Birth certificate * Marriage certificate * Social Security card * Court decree of a legal name change |
| Address | * Unexpired driver’s license * Unexpired state ID * Utility bill\* * Mobile phone bill\* * Pay stub\* * W-2 from the year immediately prior * 1099 from the year immediately prior * Current rental agreement or mortgage statement * Property deed * Bank statement\* |
| SSN | * Social Security card * W-2 form * 1099 form * Federal tax transcript * Pay stub if it lists a SSN |
| Date of Birth | * Driver’s license * State ID * Passport |

\*Document must be dated within 60 days of the application date.

Finally, TransUnion may have a risk output of “fail”. In this instance, the loan application cannot proceed until the applicant remediates the matter directly with the credit bureau.

The nature of a mobile lending platform is such that applicants will not appear in person in a traditional brick and mortar financial institution. Due to this, applicants are also required to upload either a driver’s license, state ID, Military ID, or Passport into the App. The photo identification provided is then matched to the individual making the loan application *either* by utilizing facial recognition software via a “selfie” or by prompting them to correctly answer a KBA question. If the applicant has previously correctly answered a KBA question, the photo identification will be accepted without the need to do so again.

If the applicant is unable to pass verification, iCW will not form a customer relationship with the applicant.

# RECORDKEEPING

iCW retains all CIP information for a minimum five (5) years after the date the account was closed, in a manner consistent with the *iCW Data Handling and Retention Policy*. CIP records are retained on a secure Amazon Webservice database (Database).

Information retained in the Database must include –

* Customer name; date of birth; and physical address
* Customer SSN
* Whether the photo identification produced is a passport, military ID or state driver’s license/state ID
* Whether the customer has opted to utilize the facial and vocal recognition features of the application (a description of non-documentary methods used to verify the identity of a customer)
* If applicable, a description of the resolution of any substantive discrepancy discovered when verifying identifying information

# COMPARISON WITH GOVERNMENT LISTS

The Office of Foreign Assets Control (OFAC) requires that all persons and entities in the United States block of freeze property, payment of any funds, transfers, and transactions with anyone on OFAC watchlists. Accordingly, iCW will not fund an account until further investigations reveals that the “hit” on the list is not a legitimate match.

To comply with this requirement at onboarding, iCW utilizes TransUnion’s OFAC Name Screen service, which screens consumer information against the following watchlists:[[1]](#footnote-1)

* Specially Designated Nationals (SDN)
* Specially Designated Terrorist (SDT)
* Specially Designated Kingpins (SDNTK)
* Foreign Sanctions Evaders (FSE)
* Foreign Terrorist Organization (FTO)
* Palestinian Legislative Council (PLC)
* Specially Designated Narcotics Traffickers (SDNT)
* Specially Designated Global Terrorist (SDGT)

TransUnion compares consumer name and date of birth against the aforementioned watchlists for potential matches and generates OFAC alerts if there is an 85 percent degree of matching or greater.

What this means is that the matching logic utilized by TransUnion will detect certain misspellings or other incorrectly entered text, and will return near, or proximate matches. This 85 percent threshold is also referred to as a minimum name score.

**Due Diligence**: Given that the minimum name score is placed at 85, if TransUnion’s software detects a possible match, TransUnion will place an OFAC alert on the credit report and remit to Lending Solutions, Inc. (LSI) to determine whether it is a legitimate match.

LSI will either disposition a TransUnion OFAC alert as a “true match” or a “false positive” by manually checking the information contained within an OFAC list against information provided by the applicant. Regardless of the outcome, all OFAC alerts dispositioned by LSI must be shared with iCW immediately upon receipt and disposition.

In the event that LSI deems the match legitimate, the BSA/AML Manager (or a designee) at iCW will perform further due diligence using LexisNexis and information obtained via iCW’s Customer Identification Program (CIP). If the BSA/AML Manager believes that the individual is on an OFAC list, they must inform WebBank via Salesforce within one (1) business day of receiving the LSI disposition.

iCW will investigate all details surrounding the attempt to acquire a loan to ascertain if a Suspicious Activity Report is also required in accordance with the *Suspicious Activity and Reporting Procedures*

Instances of legitimate list matches are retained for five (5) years for audit and regulatory purposes.

# CUSTOMER NOTICE

The following notice regarding CIP is embedded with the iCW application, which is available for customer review prior to officially opening an account:

In accordance with Section 326 of the USA PATRIOT Act signed October 26, 2001, all financial institutions are mandated to implement a Customer Identification Program (CIP) as a tool to protect the U.S. financial system from money laundering, terrorist financing, identity theft and other forms of fraud. iCreditWorks is required to: \*Obtain customer identifying information from each customer prior to account opening and in identifying signatory individuals added to an existing or new account. \*Maintain records of the information used to verify the person’s identity including name, address and other identifying means. In all cases protection of our customer’s identity and confidentiality is iCreditWorks pledge to you. We proudly support all efforts to protect and maintain the security of our customers and our country.

# TESTING PROCEDURES AND CONTROLS

**Independent testing**: Annually, iCW will support WebBank to secure the services of an independent third party with credible industry experience to test its CIP procedures and controls at least once every calendar year as part of the iCW’s overall obligation to engage an independent party to audit its overall compliance program.

The independent testing report will include the name or qualifications of the independent auditor; objective and scope of the review; procedures performed, and transaction testing completed; and findings or recommendations identified including management’s response. Any violations, policy or procedure exceptions, or other deficiencies and recommendations noted during the review will be reported in a timely manner to the iCW Board. The Board, through the Chief Compliance Officer, will track audit report findings and implement and document corrective actions.

**Internal Review**: At least once a year, iCW will provide a report to WebBank on the overall effectiveness of its Customer Identification Program. The report provided to the Bank by iCW will contain a write-up covering:

* The effectiveness of these Procedures in assessing customer identity;
* Service provider arrangements;
* Significant breaches of procedure and management response; and
* Recommendations for needed changes in the Customer Identification Program.

# ROLES AND RESPONSIBILITIES

Chief Compliance Officer:

* Oversee and provide guidance to the overall administration to the CIP
* Review and approve changes to the CIP Procedures

BSA/AML Manager:

* Updates the CIP Procedures
* Dispositioning alerts from relevant government lists (ascertains whether an alert or match is legitimate)

1. **dOCUMENT mANAGEMENT**

iCW will maintain the Procedures and supporting documentations in accordance with the *iCW Data Handling and Retention Policy*. iCW will ensure all employees understand their obligations in retaining documents and are aware of the processes for retention and disposal of records.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Modified Date** | **Modified By** | **Approved By** | **Revision** | **Version** |
|  |  |  |  |  |

|  |  |  |
| --- | --- | --- |
| **Approved Date** | **Approved By** | **Version** |
| July 22, 2020 | WebBank | 1.0 |

1. *See* the Watchlist Procedures for OFAC compliance measures taken after onboarding [↑](#footnote-ref-1)