

**Fraud Prevention Procedures**

|  |  |
| --- | --- |
| Procedure Owner: Cristian Mandachescu | Version: 1.0 |
| Written by: Cristian Mandachescu | Effective Date: 4/9/2020 |

Table of Contents

[1. Purpose and Scope 3](#_Toc37321838)

[2. Related Documents 3](#_Toc37321839)

[3. Definitions 3](#_Toc37321840)

[4. Procedures 4](#_Toc37321841)

[5. Roles and Responsibilities 6](#_Toc37321847)

# Purpose and Scope

* 1. **Purpose**

These procedures govern fraud prevention for iCreditWorks Mobile Platform at the Applicant, Device and Documentation level. This comprehensive approach covers verification of the user’s mobile phone number, device, IP address, email address, in addition to CIP, OFAC and income verification.

* 1. **Scope**

These procedures apply to all users of the iCreditWorks Mobile Platform during the application and servicing process.

# Related Documents

These Procedures supplement and should be read in conjunction with **iCreditWorks’ *Credit Policy***, ***Credit Standard Operating Procedures,******Servicing Procedures Overview, Customer Identification Program Procedures, User Identification Procedures and the Identity Theft and Red Flags Procedures****.*

# Definitions

**Applicant:** A consumer who is seeking a loan under the iCreditWorks loan program as primary borrower or co-borrower and, as such, whose name appears on the credit application and whose income and credit history are used to qualify for a loan.

**iCreditWorks Mobile Platform**: The consumer-facing iCreditWorks mobile interface used to facilitate the credit application process and, once the loan is funded, loan payments, inquiries and other administrative activities during the life of the loan.

**Device ID:** A unique identifying ID with which a mobile device can be identified uniquely across the globe.

**IP Address:** An Internet Protocol address (IP address) is a numerical label assigned to a User’s mobile phone.

**Identity:** Identification of a user using a govt issued valid ID like driver’s license or passport.

**User**: An individual who registers as a user of the iCreditWorks Mobile Platform, including Applicants and Other Registered Users.

**Other Registered User:** An individual, other than the borrower or co-borrower, who registers to use the iCreditWorks Mobile Platform after a loan is funded. Other Registered Users include users authorized to access a loan account by the borrower (i.e., an authorized user), power of attorney holders, or third parties alleging fraud.

# procedures

Any individual seeking to use the iCreditWorks Mobile Platform must download the app to their mobile phone and enter their mobile phone number. Fraud Procedures are performed on the User (Applicant or Borrower), Device (mobile device used) and Documentation uploaded by the user as following:

**Process:**

* Device data elements are collected from the user’s device through a TransUnion (TU) SDK (software development kit) once the User downloads the iCW App
* Identity and income data elements are entered by the user on the first screen: Name, DOB (date of birth), SSN, Address, Income, Mobile Phone Number
* iCW connects with TU services (iovation/ID Vision) to verify all data elements collected from the user and user’s device. If there are discrepancies in the information collected or indications that the user or device have been involved in fraudulent activity, the user is asked to upload Government issued ID and/or other documentation and additional checks are performed:
  1. Government ID is authenticated by Lexis Nexis and the information extracted from the document is cross referenced
  2. Knowledge Based Authentication (KBA) is initiated by Lexis Nexis if the ID verification process is not satisfactory
  3. Other documentation is authenticated as described in this document and related documents and the information extracted is cross referenced against information obtained from other sources
* iCW also connects with TU to obtain a credit report and other underwriting information to validate the identity and income of user. If there are discrepancies with respect to CIP or income, the user is asked to upload documentation and additional checks are performed as described in this document and related documents
* iCW performs an OFAC check based on information received from TU (IDVision)
* iCW asks pre-approved applicants to register in order to finalize the approval and users need to provide a valid email address that is verified during the process
* As part of the registration process, iCW asks users to take a selfie using the tool embedded in the iCW app, and then uses Lexis Nexis to match the selfie to the photo in the ID by doing a multipoint biometric verification
* If the user selects not to provide a selfie, then KBA is initiated using Lexis Nexis
* To complete the loan approval process, iCW asks the dental partners to validate that the user is the patient they treat, based on either the selfie or a picture extracted from their Government ID, and that the amount requested is aligned with the required payment for the treatment
* The dental provider is asked to confirm the beginning or completion of treatment before the loan amount is disbursed to the dental provider. The user is notified when the dental provider confirms that treatment was initiated or completed
* If the user selects AutoPay, when the user connects his/her account we confirm that the user is owner or part-owner of that account

**User verification procedures** are automatically performed when an individual attempts to register as a User or when a registered User attempts to change this information in their User Profile. These procedures are described in the User Identification Procedures. If a discrepancy is identified, the User is prevented from proceeding with the registration process or the user profile change.

For **Documents verification**, procedures combine algorithmic checks with reviews conducted by fraud specialists and are performed by iCW and its partners: Ocrolus and LSI. They include:

* Image Alteration Detection that automatically recognizes photoshopped and fabricated documents
* Data Tampering Detection that leverages document metadata and harnesses fraud specialists and a business intelligence network with hundreds of other financial services that collaborate to stop bad actors and get ahead of the latest methods used by fraudsters

**KBA Authentication**

This configuration helps confirm a subject's identity by generating knowledge-based authentication questions that typically only an identity owner would know. In addition, authentication can dynamically adapt the difficulty level of a quiz based on certain high-risk events or business rules, as well as automatically adjust for minor input errors, name variations, and inconsistencies in public data.

**Email Risk Assessment**

This configuration analyzes the subject's input email address for fraud risk.

**ID Verification**

This configuration recognizes and validates government-issued IDs. The service captures the data from base64-encoded images of the ID, analyzes the graphic security elements for accuracy, and delivers the authentication results.

**Verification of Income**

Verification of income is completed by comparing the stated income to an income estimate model provided by TransUnion’s “Credit Vision Income Estimator” (CVIE). If the stated income is no more than 125% of the CVIE income, or it is less than the CVIE income, the stated income will be used to calculate a debt to income ratio without any additional requests for supporting documentation. If the stated income is more than 125% of the estimated income and if the applicant does not qualify for the loan using the lower estimated income from TransUnion, Company requests the applicant to provide proof of income using paystubs, w-2s or tax returns. If Company is unable to verify income, the loan will be declined, and an adverse action will be given within 30 days of the application.

**IDVision**

TransUnion’s ***IDVision Alerts*** facilitates compliance with sections of the Red Flags and Know-Your-Customer regulations and reduces fraud exposure by pinpointing identity and identity element misuse that may lead to payment defaults, chargeoffs and fraud-related costs. These TransUnion solutions can help detect true name and synthetic fraud, application velocity, identity relational and behavioral anomalies, SSNs belonging to deceased persons or minors,

consumer statements on credit files, identity verification issues, Social Security Number issuance and misuse, address misuse, etc. Alerts returned are based on the input and/or file-based identity elements. For launch, iCW will use the best-practice settings available for this solution, and, after launch, will configure each alert individually to help meet specific fraud, compliance and identity verification strategies based on real data. There are eighty-one (81) alerts available in the IDVision solution. The alerts are based on the consumer identity element (Social Security number, address, and telephone number) and subject matter content (consumer alerts and product status). For each alert, a risk level is provided based on industry best practices to assist in determining the associated risk as well as potential follow-up strategies. The risk levels are categorized as Red, Amber or Green, depending on the number and level (high/medium/low) of alerts.

**Other Verifications**

This configuration can help confirm the accuracy of subject-provided identity information (for example, name, address, phone, and DOB (date of birth). Verification checks whether the data about the subject matches the data that is collected from public records and other data sources. Verification can also identify potentially high-risk situations (for example, PO Box addresses or an SSN that is associated to a deceased person).

# Roles and Responsibilities

| **Responsible Party** | **Roles** |
| --- | --- |
| iCW Chief Risk Officer | * Responsible for overseeing the implementation of this procedure and for approving any changes/enhancements to this procedure. |
| iCW Chief Information Security Officer | * Responsible for monitoring implementation with respect to mobile application user security protocols and identifying opportunities to enhance these procedures. |
| WebBank | * Responsible for reviewing proposed changes to this procedure. |
| iCW Head of Underwriting | * Responsible for ensuring the accuracy/currency/validity of the procedure. |