OneSumX Customer Due Diligence

Red Flag Quick Start Guide

July, 2018
Copyright Information

© 2018 Wolters Kluwer, Inc., St. Cloud, Minnesota. All rights reserved.

Published in July, 2018.

Printed in the United States of America.

The reproduction of this material is strictly prohibited. Information is subject to change without notice and does not represent a commitment on the part of Wolters Kluwer, Inc. The software described is furnished under a license agreement and may be used or copied only in accordance with the terms of the agreement.

Legal Counsel

In developing this program, online documentation, printed manuals, forms, and documents we have interpreted the various laws, regulations, and commentary. We cannot and do not guarantee that our interpretations are correct, except as is stated in the license agreement.

Law requires the following notice:

THE PRODUCTS AND SERVICES OF WOLTERS KLUWER, INC. ARE NOT A SUBSTITUTE FOR THE ADVICE OF AN ATTORNEY.

We encourage you to seek the advice of your own attorney concerning the use and legality of this program, documentation, and forms. If your interpretations or your counsel’s interpretations are contrary to ours, you should, of course, follow your own interpretations in using this program, documentation, and forms.

Version

Document version 5.6.60
# Table of Contents

Table of Contents ............................................................................................................................................. 3

Introduction to Red Flag Requirements ........................................................................................................... 4
  Background and Legislative Overview .................................................................................................................. 4
  Program Requirement ....................................................................................................................................... 4

Identifying Relevant Red Flags .......................................................................................................................... 4

Detection of Red Flags ....................................................................................................................................... 5

Categories of Red Flags .................................................................................................................................... 5

Appropriate Response ......................................................................................................................................... 5

Updating Program ............................................................................................................................................... 6

Training and Administration ............................................................................................................................... 6

Address Discrepancies ....................................................................................................................................... 6

Reasonable Policies and Procedures .................................................................................................................. 7

Software Detection ............................................................................................................................................. 8

Using OneSumX Customer Due Diligence to Detect Red Flags ..................................................................... 8
  Identity Verification .......................................................................................................................................... 8

Identity Authentication ........................................................................................................................................ 10

Other Services .................................................................................................................................................... 11

CDD Service ....................................................................................................................................................... 11

Beneficial Ownership Certification service ...................................................................................................... 11

QualiFile and Deluxe Detect ............................................................................................................................. 11

OFAC .................................................................................................................................................................... 11

Reporting and Query Function ............................................................................................................................ 12

Available Support Resources ............................................................................................................................. 12

OneSumX Customer Due Diligence User Guide ............................................................................................... 12
  Contacting Software SupportLine ..................................................................................................................... 12

Internet ................................................................................................................................................................. 12

Phone ................................................................................................................................................................. 12

E-Mail ................................................................................................................................................................. 12

Appendix A: Red Flag Examples .......................................................................................................................... 13

Red Flags and Detection .................................................................................................................................... 13
OneSumX Customer Due Diligence FACT Act Red Flag Quick Start Guide

Welcome to the OneSumX Customer Due Diligence FACT Act Red Flag Quick Start Guide. This document is intended to provide users of the OneSumX Customer Due Diligence software application with information relevant to the FACT Act and Red Flag requirements and how to use the software to comply with the regulations set forth by the FACT Act.

Introduction to Red Flag Requirements

Background and Legislative Overview

Red Flag requirements come from sections 114 and 315 of the Fair and Accurate Credit Transactions (FACT) Act, enacted in December 2003. This legislation amends the Fair Credit Reporting Act. Final FACT Act regulations were issued October 31st, 2007 and were effective as of January 1, 2008. Compliance with the regulation was mandatory starting November 1, 2008.

Three regulations were defined as part of the legislation.

- Identity Theft Prevention Program
- Address Discrepancy Requirement
- Requirements for Card Issuers

Program Requirement

- Each financial institution or creditor that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program.
- Must be designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.
- The Program must be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

Identifying Relevant Red Flags

- Need policies and procedures for identifying which Red Flags are relevant to detecting identity theft.
- Section II of the guidelines contains a list of factors that a financial institution or creditor should consider as appropriate.

These factors are:

- The types of covered accounts offered or maintained;
- The methods provided to open covered accounts;
- The methods provided to access covered accounts; and
- Previous experiences with identity theft.
Detection of Red Flags

- Program must contain reasonable policies and procedures to detect the Red Flags that a financial institution has incorporated.
- Section III of the guidelines provides examples of various means to detect Red Flags.
- In connection with the opening of accounts, may obtain identifying information about, and verify the identity of, a person opening the account, for example, using the policies and procedures on identification and verification from the CIP rules.
- In connection with existing accounts, may authenticate customers, monitor transactions, and verify the validity of change of address requests.

Categories of Red Flags

- Alerts, notifications or warnings from a Consumer Reporting Agency
- Suspicious documents
- Suspicious personal identifying information
- Unusual use of, or suspicious activity related to, the covered account
- Notice from customers, victims, law enforcement, or other persons regarding possible identity theft

Appropriate Response

- Respond appropriately to any Red Flags detected to prevent and mitigate identity theft.
- In order to “respond appropriately,” your institution must assess whether the Red Flags that are detected evidence a risk of identity theft, and need a reasonable basis to conclude that a Red Flag does not evidence a risk of identity theft.
- Your policies and procedures should provide for appropriate responses to the Red Flags that your institution has detected that are commensurate with the degree of risk posed.
- In determining an appropriate response, your institution should consider aggravating factors that may heighten the risk of identity theft.
- How do you document your detection and response?

Appropriate responses may include the following (examples):

- Monitoring an account for evidence of identity theft.
- Contacting the customer.
- Changing passwords, security codes, or other devices that permit access to an account.
- Reopening an account with a new account number.
- Not opening a new account.
- Closing an existing account.
- Not attempting to collect on an account or not selling a covered account to a debt collector.
- Notifying law enforcement.
- Determining that no response is warranted.
Updating Program

- Must update the program (including the Red Flags determined to be relevant) to reflect changes in risks to customers and to the safety and soundness of your institution from identity theft
- Only requires “periodic” updating
- Section V of the guidelines gives guidance

Factors that should cause program updates include:

- Your experiences with identity theft,
- Changes in methods of identity theft,
- Changes in methods to detect, prevent, and mitigate identity theft,
- Changes in accounts that you offer or maintain, and
- Changes in business arrangements

Training and Administration

- Involve the board of directors, a committee of the board or an appropriate senior management employee in the oversight, development, implementation and administration of the plan;
- Obtain approval of the initial written program from either the board of directors or an appropriate committee of the board;
- Train institution staff as necessary to implement the program in compliance with the requirement for training; and review and exercise oversight of service provider arrangements.

Address Discrepancies

- This applies to a user of consumer reports that receives a notice of address discrepancy from a consumer reporting agency,
- The notice informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address in the agency’s file for the consumer.
- Must develop and implement reasonable policies and procedures designed to enable you to form a reasonable belief that a consumer report relates to the consumer about whom you requested the report.
Reasonable Policies and Procedures

- Comparing the information in the consumer report provided by the consumer reporting agency with information that you:
  - Obtain and use to verify the consumer’s identity in accordance with the requirements of the CIP rules;
  - Maintain in your own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
  - Obtain from third-party sources; or
- Verifying the information in the consumer report provided by the consumer reporting agency with the consumer.
Software Detection

OneSumX Customer Due Diligence is a useful tool to assist your organization with the detection of red flags. The services available within the software application help to perform several different types of red flag detection.

Using OneSumX Customer Due Diligence to Detect Red Flags

OneSumX Customer Due Diligence provides a set of flexible tools that automate your identity verification operations from account opening to record archiving. OneSumX Customer Due Diligence streamlines your workflow and ensures compliance by verifying individual and business identities and screening applicants and account holders against government watch lists.

OneSumX Customer Due Diligence utilizes a uniquely comprehensive 3 type verification process that includes:

- **Positive Verification – Confirms that presented information is accurate.**
  Positive verification ensures that information provided by applicant matches information available from trusted third party sources. You can verify an applicant’s identity by comparing their answers on application questions against information in a trusted database to see if the information supplied by the applicant matches information in the database.

- **Logical Verification – Confirms that presented information is logically consistent.**
  Logical verification is a means of cross checking the information provided for consistency. Frequently an identity thief will want to combine some actual identity information obtained from a victim with information such as an address or phone number that the identity thief controls. Logical verification helps to flag such efforts to combine information.

- **Negative Verification – Confirms that customer is not on watch lists.**
  Negative verification ensures that information provided has not previously been associated with fraudulent activity. For example, applicant information can be compared against fraud databases to determine whether any of the information is associated with known incidents of fraud.

OneSumX Customer Due Diligence is, therefore, a useful combination of software tools to use that will assist in the detection of red flags.

Identity Verification

The Guidelines for Detecting Red Flags say that you should address detection for new accounts by means such as:

“Obtaining identifying information about, and verifying the identity of, a person opening a covered account, for example, using the policies and procedures regarding identification and verification set forth in the Customer Identification Program rules”

So, the use of a CIP verification solution like OneSumX Customer Due Diligence Verification is specifically made an option. OneSumX Customer Due Diligence Identity Verification service is a combination of positive, negative, and logical verification to use to detect red flags.
**What is Match Comparison?**

OneSumX Customer Due Diligence’s Identity Verification service uses match comparison to return results. What this means is that the service compares the data you enter for a given individual against published data and determines whether the data provided by the individual matches. If the data matches, the individual is less likely to be a risk. If there’s a mismatch of data, it is an indication, or red flag, that the individual should be researched more thoroughly. Obtaining a “match” in the results field of your result report indicates a level of positive verification for that piece of information (name, address, date of birth, etc.).

**Workflow**

After you have run ID Verification checks on individuals, and you receive the results of the verification, you have the option to include any supporting comments regarding the results, including the opportunity to explain any of the results. From there, you decide whether to complete or reject the results based on your analysis.

**Understanding Warning Messages**

Warning messages available in the ID Verification service are intended to provide you with additional detail regarding the information.

Some of the warning messages are of the negative verification type, such as:

- Deceased identity
- Social, address, driver’s license or phone invalid
- Known fraud address
- Prison, mail delivery, or check cashing address; and
- Social issued before birth, recently issued or issued after age 18.

Some of the warning messages are of the logical verification type, such as:

- Phone reported with differing names or addresses
- Social reported with differing names or addresses
- Address or phone given for an individual is actually for a business; and
- Name not reported at address

Sometimes mismatches are inconsequential, such as when the individual has changed their name, especially when a change in marital status has occurred. Other times, mismatches are much more significant warnings and warrant further investigation. For example, if a name or address is an obvious mismatch without a logical explanation.

Included in Appendix A is a list of the 26 illustrative examples from the Red Flag regulations and how some of the OneSumX Customer Due Diligence warning messages might be indicators of those red flags. Some of the red flag examples lend themselves to manual detection by use of a consumer report or by review of an identification document, but for those cases the use of ID verification, authentication or other tools may serve the purpose of providing additional data for use in confirming whether identity theft may be indicated.
Completing a Review

To complete a review and accept the results returned by the ID Verification service, click Complete. This action saves and records the results.

Rejecting a Review

In some instances you may wish to reject a review if you believe you have sufficient reason to explain any identified mismatches. Be sure to enter any specific comments regarding your justification for the rejection so they may be archived and provide a paper trail in the future.

Identity Authentication

Identity Authentication is another service available within OneSumX Customer Due Diligence.

The Authentication service is designed to produce a series of questions for a given set of identification data that only the individual being processed should know. The Authentication process relies on numerous identity and validation databases to gather the relevant records for evaluation, providing for greater confidence that the questions asked (and available answers) are relevant and appropriate for the person on whom they are based.

Authentication is a tool that is particularly valuable for detection of identity theft in existing accounts. The Guidelines for Detecting Red Flags mentions such detection by suggesting:

“Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.”

In addition, authentication is mentioned in red flag number 18 in the red flag illustrative examples which reads as follows:

“18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.”

Using Out-of-Wallet Questions to Validate

The purpose of an Authentication service is to provide a more thorough analysis of the individual in question. Authentication provides that analysis by going beyond matching information generally available in a wallet or on a consumer report and instead poses challenge questions to the individual. These questions are greater reaching than the match detection service provided by ID Verification in that the material presented reflects a broader background. For example, an individual may be asked which one of four previous addresses provided is correct or to identify which of the states provided was actually the one in which their SSN/TIN was issued in.

Out-of-Wallet Questions and Results Logging

Users of the OneSumX Customer Due Diligence Authentication service work with the individual applicant to answer these questions and then log the investigation results in the application. The software then returns the results, which lists which of the challenge questions were answered correctly and which were answered incorrectly. Incorrectly answered questions should be considered a potential red flag.
Completing or Rejecting a Review

To complete a review, you must determine whether you believe the person is indeed the person they claim to be. You have the option to complete or reject a review.

You may provide additional comments to include with the results. For example, if you have taken measures to accurately identify information the Authentication service flagged as incorrect, and decide to accept the individual or entity, you may use the comments section to indicate your rationale for not rejecting the application.

Other Services

Several other verification or list checking services are available in OneSumX Customer Due Diligence that can be used in conjunction with verification and authentication:

CDD Service

The CDD service available in OneSumX Customer Due Diligence is a question-asking process completed at the time of account opening and is used to assign a risk score to a potential customer. This type of assessment is used to determine a risk factor for a given individual based on the elements contained within the questions.

Refer to OneSumX Customer Due Diligence User Guide for specific instructions on working with the Customer Due Diligence service in both the CDD User Guide and Administrator’s Guide respectively.

Beneficial Ownership Certification service

The Beneficial Ownership Certification service is used to comply with the FinCEN CDD Final Ruling originally issued in 2016, with an effective implementation date of May 11th, 2018. This service is used to collect information regarding business entities and individuals, such as Beneficial Owners of the business entity, the Managing Authority for the business and the individual opening the account on behalf of the business. The intention of the ruling is to collect these names with the business entity as part of a certification process that also performs a verification/validation of the business entity and associated individuals.

The verification/validation aspect of the ruling may be satisfied by running other services within OneSumX CDD such as ID Verification and OFAC as examples. It is the responsibility of the institution to determine how this aspect of the ruling is to be fulfilled.

QualiFile and Deluxe Detect

Two additional services, QualiFile and Deluxe Detect may also be used to provide verification for an applicant. Refer to the OneSumX Customer Due Diligence User Guide for instructions on working with these services.

OFAC

The Office of Foreign Assets Control, or OFAC, administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers.

The OFAC service checks your customer data to determine whether or not your customer potentially matches any of the individuals or entities on the published OFAC lists.

Refer to the OneSumX Customer Due Diligence User Guide for instructions on working with this service.
Reporting and Query Function

The OneSumX Customer Due Diligence Query function can be used to run a management summary report of all records run against a selected service and/or decision for a specified period of time to show which applicants may have been rejected due to Red Flag violations.

Available Support Resources

OneSumX Customer Due Diligence User Guide

The OneSumX Customer Due Diligence User Guide can be found within the application in the Help tab. This guide will provide more specific instructions on how to use the various services.

Contacting Software SupportLine

Internet

You can visit us on the Internet at www.wolterskluwerfs.com.

Phone

Our support staff is available Monday through Friday; 7 A.M. to 7 P.M. Central Time. Voice mail operates 24/7, allowing you to leave us a message at any time convenient to you, and our SupportLine personnel will return your call within 72 hours. To help us handle your question as quickly as possible, please have these items available before you call:

- product name and version number
- customer number

E-Mail

To contact Wolters Kluwer through email, submit all requests to:

OneSumXCDD.Support@wolterskluwer.com
Appendix A: Red Flag Examples

Red Flags and Detection

This table provides 26 Red Flag examples and how OneSumX Customer Due Diligence may be used as part of their detection.

<table>
<thead>
<tr>
<th>Red Flag</th>
<th>How Detected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud or active duty alert received</td>
<td>Consumer report – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Notice of credit freeze received</td>
<td>Consumer report – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Notice of address discrepancy received</td>
<td>Consumer report – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Unusual pattern of account activity detected</td>
<td>Consumer report – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Altered or forged identification documents provided</td>
<td>Review of document – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Photo or ID information is not consistent with the appearance of the applicant</td>
<td>Review of document – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Information on the identification is not consistent with information provided</td>
<td>Review of document – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Information on the identification is not consistent with information on file</td>
<td>Review of document and customer information file – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Application altered, forged or destroyed and reassembled</td>
<td>Review of document – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Personal information provided is inconsistent with external information</td>
<td>Decreased identity found with full name match AS01, Decreased identity found with last name match AS02, Decreased identity found with no name match AS03, Social issued before birth AS04, Social issued in last three years AS05, Social issued after age 18 AS06, Address invalid FA01, Driver's License is invalid in state FL01, Phone invalid FP01, Social invalid FS01, Name not reported at address</td>
</tr>
<tr>
<td>Red Flag</td>
<td>How Detected</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Personal information provided is internally inconsistent.</td>
<td>Phone and zip code mismatch AP06, Name not reported at address VA01, Phone reported only with different first name(s) VP02, Phone reported only with different last name(s) VP03, Phone reported only with different address(es) VP04, Social reported only with different first name(s) VS02, Social reported only with different last name(s) VS03, Social reported with last name and other name(s) VS04, Social reported only with different address(es) VS05</td>
</tr>
<tr>
<td>Personal information provided is associated with known fraudulent activity.</td>
<td>Known fraud address AA16</td>
</tr>
<tr>
<td>Personal information provided is of a type associated with fraudulent activity.</td>
<td>Prison Address AA01, Temporary Address AA02, Mail delivery address AA03, Business address AA05, Check Cashing outlet address AA15, Phone listed to a prison AP01, Phone listed to a temporary address AP02, Phone listed to a mail delivery location AP03, Phone is cellular or mobile AP04, Phone is listed to a business AP05, Phone is listed to</td>
</tr>
<tr>
<td>Red Flag</td>
<td>How Detected</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------------------------------</td>
</tr>
<tr>
<td>New revolving credit account used in a manner associated with fraud.</td>
<td>Account monitoring – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Account used in a manner inconsistent with established patterns of activity</td>
<td>Account monitoring – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Account inactive for a long period of time is used</td>
<td>Account monitoring – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Mail returned as undeliverable but transactions continue</td>
<td>Account monitoring – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Notice received that customer is not receiving paper account statements</td>
<td>Notice from customer – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Notice of unauthorized account charges or transactions received</td>
<td>Notice from customer – follow up with Verification/Authentication</td>
</tr>
<tr>
<td>Notice received that account is for a person engaged in identity theft</td>
<td>Notice from customer or other party – follow up with Verification/Authentication</td>
</tr>
</tbody>
</table>

Table 1. Red Flag Detection Criterion

⚠️ **User Note:** There may be returned messages that do not correlate with being a red flag.