

COMPLYID RED FLAG AND ID VALIDATION SERVICES

CSC

AT A GLANCE

- Automatically Detect More Than 200 Credit Report Red Flags and ID Discrepancies
- Customize Detection and Resolution Options to Your Specific Risk Policy
- Rapidly Investigate ID Discrepancy and Red Flag Conditions
- Resolve Operational Bottlenecks
- Support In-House Identity Theft Prevention Initiatives
- Produce Detailed Audit Trail to Demonstrate Compliance and Track Plan Performance

Take an End-to-End Approach to Detecting, Resolving and Tracking Red Flags

Creditors across a wide range of industries are struggling with strategies to meet the Red Flag regulations of the FACT Act, which went into effect on Nov. 1, 2008. The potential impact to workloads is significant. The act applies to any creditor that offers or manages accounts involving multiple payments for personal, family or household purposes. CSC estimates that more than 30 percent of all applications will generate red flags across multiple lines of business.

CSC has developed a set of Web-based software products and services for an end-to-end approach to managing FACT Act compliance, regardless of the type of credit you're providing. ComplyID™ Red Flag and ID Validation Services automatically detect more than 200 credit report red flags as well as other alerts related to ID discrepancies.

Upon detection, ComplyID automatically verifies, validates and resolves discrepancies through multiple data sources. When needed, a real-time interactive question-and-answer authentication option is also available. ComplyID scores the results consistently with your credit rules and risk policies. This approach helps your staff quickly resolve ID issues and removes processing bottlenecks.

Integrate with Your Identity Theft Prevention Program

ComplyID offers more than just handling of red flags. It equips your staff with a powerful toolkit to quickly analyze and resolve processing delays. ComplyID incorporates and helps to enforce your ID theft prevention program and risk policies, ensuring a standardized approach to ID validation across multiple lines of business. ComplyID supports a full range of accounts:

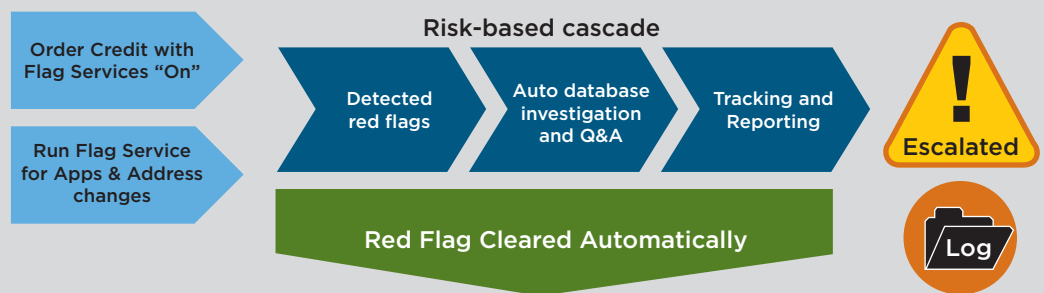
- Mortgages and equity loans
- Check and deposit accounts
- Credit and debit cards
- Utility, cell phone, commercial
- Automotive
- Medical, hospital, clinic and more.

Ensure Detailed Tracking and Reporting

ComplyID gives you advanced tracking and reporting capabilities to facilitate your compliance with FACT Act regulations. Detailed reports on issues and resolutions will help you identify trends and fine-tune your program to meet your organization's specific needs.

For more information about CSC's ComplyID Red Flag and ID Validation Services, call 866.477.6651 or send an e-mail to ncd@csc.com.

CSC Automated Red Flag Evaluation Service



Detect

- ✓ Detect red flags on credit report & apps
- ✓ Check for inconsistencies between name, address, phone, SSN, DOB, Drivers Lic info.
- ✓ Check for high risk name, address, etc.

Investigate & Score

- ✓ Return risk score & details
- ✓ Automatically return Q&A for instant resolution with consumer
- ✓ Alert client on status change

Track

- ✓ Audit log of all red flags & steps taken
- ✓ Management alerts
- ✓ Performance reports
- ✓ Training site for employees

Red Flag Legislation Overview

On November 1, 2008, as a part of the ongoing effort to stem identity theft, the joint financial regulatory agencies (FTC, FDIC, Comptroller of the Currency, OTS, OCC, Federal Reserve System Board, and NCUA), have modified the FACT Act to add compliance measures to deal with identity theft in creditor operations. This legislation is known as the "Red Flag" legislation and it applies to companies that offer or maintain a covered account.

A Covered Account is (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft. Covered Accounts include credit card accounts, mortgage loans, automobile loans, margin accounts, cell phone accounts, utility accounts, checking accounts, and savings accounts. A Covered Account may also be a commercial account for which there is a foreseeable risk of identity theft - for example, small business or sole proprietorship accounts.

In addition to traditional financial institutions and creditors, any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit must comply as well. This includes hospitals, clinics, finance companies, automobile dealers, mortgage brokers, utility companies, telecommunications companies, and non-profit or governmental entities if payment for goods or services is deferred.

If the Red Flag Rules apply to your organization you must develop, adopt, and implement a written Identity Theft Prevention Program. This Program must be managed by the Board of Directors or senior employees of the financial institution or creditor and contain policies and procedures to:

- ✓ Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program. Red Flags fall into the following suggested categories:
 - Alerts, notifications, or warnings from a consumer reporting agency
 - Suspicious documents
 - Suspicious personally identifying information, such as a suspicious address
 - Unusual use of - or suspicious activity relating to - a covered account
 - Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.
- ✓ Detect Red Flags that have been incorporated into the Program
- ✓ Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
- ✓ Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft
- ✓ Provide appropriate training to personnel responsible for implementing and conducting the program.

The banking and credit union regulatory agencies, as well as the FTC are charged with enforcing these regulations. Violations are punishable through injunctive relief requiring compliance and the payment of civil penalties. For questions about compliance with the Red Flag Rules, visit ftc.gov or you may contact RedFlags@ftc.gov for questions specific to your organization.

Special Requirements for Credit and Debit Card Issuers:

In addition to the red flag rules, credit and debit card issuers have a special duty to handle address changes. Now, if a card issuer receives a change of address notice, the account should be monitored for a 30 day period to determine if a new card or replacement card request occurs. If it does, the card issuer should follow reasonable policies to assess the validity of an address change prior to opening a new or replacement card. The steps may include:

- ✓ Notify the cardholder of the request at the former address
- ✓ Notify the cardholder through other means of communication previously agreed to
- ✓ Use some other means of assessing the validity of the address change in accordance with reasonable policies and procedures.

Special Handling of Address Discrepancies for Users of Consumer Credit Reports:

Credit Reporting Agencies (CRAs) have had a policy in place under FACTA requiring them to send an address discrepancy alert on a credit report when the address on the consumer's application is substantially different than the one listed on the consumer report. As a user of credit information, you must form a reasonable belief that the consumer report relates to the consumer in question whether it's a new or existing account. If you use credit information from a CRA, and there is an address discrepancy indicator, and you formed an ongoing relationship with the consumer, the regulation requires you to report back to the CRA a "confirmed address" if you normally report to the CRAs in your normal course of business. The CRAs are accommodating this requirement by allowing a creditor to place a "C" for confirmed into the Metro tape format used by the CRAs. Please contact your CSC Account Manager if there are questions around address discrepancies.

About CSC

CSC, one of the world's leading consulting and IT services firms, helps clients in industry and government achieve strategic and operational results through the use of technology. The company's success is based on its culture of working collaboratively with clients to develop innovative technology strategies and solutions that address specific business challenges. Having guided clients through every major wave of change in information technology since 1959, CSC combines the newest technologies with its capabilities in consulting, systems design and integration, IT and business process outsourcing, applications software, and Web and application hosting to meet the individual needs of global corporations and organizations.

About CSC in Financial Services

CSC distinguishes itself through its time-tested ability to plan, build and operate highly reliable, efficient and secure business and IT solutions for leading financial services firms around the world. To complement its capabilities in consulting, systems integration and outsourcing, CSC brings financial services industry knowledge and experience, a comprehensive portfolio of financial services application software and an extensive network of industry and technology partners. More than 10,000 CSC employees are dedicated to serving financial services clients, including more than 1,200 major banks, insurers and investment management and securities firms.

