
# Comprehensive Red Flags Audit Support Services

## Overview

The "Red Flags Rule" requires financial institutions and creditors to implement identity theft prevention programs that identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

On December 4, 2003, the President signed the Fair and Accurate Credit Transactions (FACT) Act into law. The FACT Act added several new provisions to the Fair Credit Reporting Act of 1970 (FCRA), including directing federal agencies to create regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances. The agencies include the Office of Currency Control (OCC), Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA) and Federal Trade Commission (FTC).

Section 114 of the FACT Act pertains to the Red Flag Regulations and Guidelines. The rules implementing section114 require each financial institution or creditor to develop and implement a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. In addition, various agencies have issued guidelines to assist financial institutions and creditors in the formulation and maintenance of a Program that satisfies the requirements of the rules. The rules implementing section 114 also require credit and debit card issuers to assess the validity of notifications of changes of address under certain circumstances.

The FTC suspended enforcement of the Red Flags Rule from November 1, 2008 until May 1, 2009 to give creditors and financial institutions additional time to develop and implement written identity theft prevention programs.

Emagined Security's Comprehensive Red Flags Audit Support Services are designed to help organizations address internal audit, state, federal, and international laws and regulations. Our services are based on a structured methodology to ensure that all auditing of an organization's compliance status is done systematically, thoroughly, and in accordance with relevant compliance regulations.

## Benefits

Our FTC Identify Theft Red Flags Audit Support Services can help you address industry and legal requirements using our structured methodology.
The following table presents Emagined Security's seven-phase methodology to manage all audit activities:

| Phase | Description |
|---|---|
| 1 | Red Flags Audit Preparation |
| 2 | Red Flags Pre-Audit Documentation |
| 3 | Red Flags Audit Management |
| 4 | Red Flags Management Remediation Support |
| 5 | Red Flags Technical Remediation Support |
| 6 | Red Flags Evidence Documentation |
| 7 | Red Flags Post Audit Support |

### Red Flags Audit Preparation

While performing Red Flags Audit Preparation, Emagined Security attends on-site meetings to gather specific audit requirements from client representatives. This is the most critical phase in the overall methodology. It is important to gather as much pertinent data as possible from key personnel and existing documents to accurately identify audit needs prior to allowing auditors to begin assessing the environment.

### Red Flags Pre-Audit Documentation

While performing Red Flags Pre-Audit Preparation, Emagined Security will document the design and create necessary support documents. The following are sample documents that may need to be created in preparation of the audit:

- Identity Theft Program Procedures
- Change of Address Procedures
- Discrepancy Program and Procedures
- Compliance Program and Procedures
- Etc.

## Red Flags Audit Management

While performing Red Flags Audit Management, Emagined Security will lead the audit on our client's behalf. During this phase, Emagined Security will help establish the scope of the audit with the auditors. This will allow the Emagined Security to govern the allowed access to systems and the infrastructure based upon the pre-defined scope. Emagined Security will work to ensure that all information gathered, including any findings, is presented from as favorable a perspective as possible to increase the probability that our client will pass the audit.

## Red Flags Management Remediation Support

While performing Red Flags Management Remediation Support, Emagined Security will perform Management Remediation Support. Upon receipt of a draft audit report, Emagined Security will identify any issues about which audit team misunderstandings or representations may exist in the Audit report. This will help to minimize any inappropriate findings that may occur when our client has in fact met audit requirements.

## Red Flags Technical Remediation Support

While performing Red Flags Technical Remediation Support, Emagined Security will perform Technical Remediation Support. Upon receipt of a draft audit report, Emagined Security will provide a detailed technical review of the audit report and assist with the technical remediation activities. In close collaboration with the client, Emagined Security technical staff will interface with Emagined Security management to develop the best approach for remediation activities.

## Red Flags Evidence Documentation

While performing Red Flags Evidence Documentation, Emagined Security will create necessary documentation needed to close out the audit findings. The following is a sample of document categories that may need to be quickly created in support of audit closure:

- Security Policies
- Compliance Documentation
- Security Architecture Documentation
- Etc.

## Red Flags Post Audit Support

While performing Red Flags Post Audit Support, Emagined Security will conduct a post-mortem phase to determine the best approach for future audits. Emagined Security will conduct a post-mortem assessment of the audit activities and resources needed to support future reviews. This review is critical to ensure that future audits are conducted in a streamlined and methodical manner. This review can also be used to provide management necessary information that will support budgetary cycles and streamlining operations.

## Level of Effort

Emagined Security can work with our clientele to develop a service offering that is tailored to their organizations needs. Duration will be dependent on the needs of the organization and modules requested. Typically, projects of this nature range from as low as 100 hours to over 1000 hours utilizing multiple consultants.

## Costing Approaches

Emagined Security offers a variety of options for performing these services including Fixed Price, Bulk Hour and Time & Material. We work with our clients to develop the best approach possible that meets their needs.