EXCHANGE | ANALYTICS

Identity Theft Prevention 2026

Course Outline

This course is designed to inform you of procedures that you and your firm can use to help identify, detect and respond to activity that may indicate a threat of identity theft or fraudulent activity related to account access. In accordance with the Identity Theft Red Flag Rules, certain financial institutions operating in the U.S. must maintain procedures designed to protect customer information and assets, as well as prevent and mitigate identity theft.

- I. Preface
    - a. Applicability to Financial Firms
    - b. Importance of Training
    - c. Importance of Identity Theft Prevention
    - d. The Prevalence of Identity Theft
    - e. Recent Examples of Notable Identity Theft
    - f. Fundamental Definitions
    - g. Course Goals
- II. Program Development, Implementation & Execution
    - a. Developing the Program
        - i. Program Requirements
        - ii. Guidance of Source of Red Flags
        - iii. Modern-Day Examples of Identity Theft Red Flags
        - iv. Categories of Red Flags
    - b. Implementation and Executing the Program
        - i. Red Flags – Category 1
            1. Notifications or Warnings from a Consumer Reporting Agency
            2. Suspicious Documents
            3. Suspicious Personal Identifying Information
            4. Unusual Use of, or Suspicious Activity Related to the Account
            5. Notice from Customers, Victims of Identity Theft, Law Enforcement Activities or Other Persons
    - c. Reminder on Illustrative Examples
    - d. Detecting Red Flags
    - e. Authentication of Customer Information for New Accounts
    - f. Procedures to Authenticate Customer Information
    - g. Verification of Address Change Requests
    - h. Preventing and Mitigating Identity Theft
        - i. Appropriate Responses to Red Flags
        - ii. Additional Responses