AMERICAN COUNCIL OF ENGINEERING COMPANIES
IDENTITY THEFT PREVENTION PROGRAM
POLICY AND PROCEDURES

POLICY

The American Council of Engineering Companies ("ACEC") strictly complies with all federal and state laws and reporting requirements regarding identity theft, including the federal Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. This policy outlines ACEC's Identity Theft Prevention Program ("Program"), which is mandated by the Red Flags Rule and governs how ACEC will (1) identify, (2) detect, and (3) respond to "red flags." A "red flag" is defined as a pattern, practice, or specific account or record activity that indicates possible identity theft.

The Program has been approved by the ACEC Executive Committee as of October 29, 2009, and the Program will be reviewed and updated by the ACEC staff at least once a year in order to ensure that the Program keeps current with identity theft risks. In doing so, the staff will consider ACEC's experiences with identity theft situations and similar experiences for other entities in the association community; changes in identity theft methods; changes in identity theft detection and prevention methods; and changes in ACEC's business arrangements with other entities. ACEC will ensure that it is using adequate and sufficient technology to protect credit card information.

It is ACEC's policy that the Vice President, Operations, is assigned the responsibility of overseeing, developing, implementing, and administering the Program. ACEC is committed to ensuring that this individual, who will act as ACEC's "privacy official" for purposes of this policy, be provided with sufficient resources and authority to fulfill these duties.

ACEC requires that its business vendors be contractually bound to protect sensitive client information to the same degree as set forth in this policy. Business vendors of ACEC who violate their agreement will be dealt with first by an attempt to address the problem, and if that fails by termination of the agreement and discontinuation of services by the business vendors.

ACEC's workforce must be trained in the policies and procedures governing compliance with the Red Flags Rule, and new workforce members are required to receive training in these matters within a reasonable amount of time after they have been hired. Should any policy or procedure related to the Red Flags Rule materially change, ACEC shall provide further training within a reasonable amount of time after the policy or procedure materially changes. All training sessions are to be documented, indicating participants, date, and subject matter.

PROCEDURES

I. Identify red flags. While providing educational and association services to members, customers, and others, ACEC may encounter inconsistent or suspicious documents, information, or activity that suggests the possibility of identity theft. The following are identified as potential red flags:

1. Notice from a member or customer, a victim of identity theft, a law enforcement agency, or someone else that an account has been opened or used fraudulently.
2. A dispute of a bill by a member or customer who claims to be the victim of any type of identity theft.
3. Suspicious documents, such as paperwork that appears altered or forged, and information on the identification that is inconsistent with other information, like a signature card or recent check.
4. Suspicious personal identifying information, such as inconsistencies with what is already known and inconsistencies in the information the member or customer has already provided.
5. Suspicious account activity, such as an account that is used in a way inconsistent with established patterns, an account that has been inactive for a long time that is suddenly used again, and information that the customer is not receiving their account statements in the mail.

II. Detect Red Flags. Employees of ACEC will be alert for discrepancies in documents and member or customer information that suggest risk of identity theft or fraud. ACEC staff will verify member or customer identity and address before educational or association services are provided and billed. Specifically, the procedures for detecting red flags are as follows:

1. When someone notifies ACEC that an account has been opened or used fraudulently, employees are required to report such notifications to their immediate supervisor and the designated privacy official. If reported to a supervisor, that supervisor should relay the information to the privacy official.
2. Regarding existing accounts, ACEC staff are expected to verify the identification of members or customers if they request information, and verify the validity of change-of-address requests and changes in banking information given for billing purposes.
3. In general, ACEC staff should be alert for the possibility of identity theft in the following situations:

    - Identifying information submitted by the member or customer appears to be altered or forged.
    - Information on one form of identification the member or customer has submitted is inconsistent with information on another form of identification or with information already in the records kept by ACEC.
    - An address or telephone number is discovered to be incorrect, non-existent, or fictitious.
    - The member or customer fails to provide identifying information or documents.
    - The member or customer signature does not match a signature in the member or customer's records.

- Any photo identification submitted by the member or customer does not resemble the member or customer, such as on-site at an educational program.

III. Respond to Red Flags. If any employee of ACEC detects fraudulent activity or if a member or customer claims to be a victim of identity theft, ACEC will respond to and investigate the situation. If potentially fraudulent activity (a red flag) is detected by an employee of ACEC:

1. The employee should gather all documentation and report the incident to his or her immediate supervisor and the designated privacy official. If reported to a supervisor, that supervisor should relay the information to the privacy official.
2. The privacy official will determine whether the activity is fraudulent or authentic.
3. If the activity is determined to be fraudulent, then ACEC should take immediate action, which may include:

    - Canceling the transaction;
    - Closing an existing membership or customer account;
    - Reopening an account with a new account number;
    - Not opening a new account;
    - Notifying appropriate law enforcement;
    - Notifying the affected member or customer; and
    - Changing any passwords or other security devices that permit access to accounts.

If a member or customer claims to be a victim of identity theft:

1. The member or customer should be encouraged to file a police report for identity theft if the member or customer has not done so already.
2. The member or customer should be encouraged to complete the ID Theft Affidavit developed by the Federal Trade Commission, along with supporting documentation.
3. ACEC will compare the member or customer documentation with personal information in the member or customer records.
4. If, following investigation, it appears that the member or customer has been a victim of identity theft, ACEC will promptly consider what further remedial act/notifications may be needed under the circumstances.
5. If, following investigation, it does not appear that the member or customer has been a victim of identity theft, ACEC will take whatever action it deems appropriate.