Data Breach Policy

Adopted: January 6, 2019

This Policy establishes how SFPE will respond in the event of a suspected or confirmed data breach involving personal identifying information (PII).

PERSONAL IDENTIFYING INFORMATION (PII) is an individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements:

a) Social security number;
b) Driver's license number; or
c) Credit card number or debit card number.

DATA BREACH ACTION PLAN

1. Any reported or suspected breach of PII data will immediately be investigated by the Society's Chief Executive Officer (CEO) and/or his or her designee. The Society will engage technology and legal experts in the process, as needed.

2. The CEO and/or his or her designee, will prepare a summary report of the breach or suspected breach as expeditiously as possible under the circumstances, that will include, but is not limited to the following information:

    - When (date and time) did the breach happen?
    - How did the breach happen?
    - What types of PII or other data were compromised? (Name, DOB, credit card information, etc.)
    - How many members/customers/employees were affected and in what jurisdictions do they reside?

3. Based on the findings of the breach investigation, the CEO will notify the Board of Directors and outside legal counsel in order to evaluate the legal and communication issues stemming from the breach, including but not limited to the following:

    - Review member, customer, or other relevant agreements, including the Society's Privacy Policy, to see whether the Society has any obligations under these agreements.
    - Identify federal, state, and international statutes and regulations potentially triggered or violated by a data breach, to see if the Society is obligated to notify the affected persons or other third parties.
    - Determine whether law enforcement or other agencies must or should be notified.

- Determine whether credit reporting agencies must or should be notified.
- Review the Society' insurance coverage to determine whether a breach incident is covered by the policy and notify the carrier, if required.

4. Based on a review from outside legal counsel, prepare appropriate notice communication, if required by law or deemed advisable. The content of a notice to affected persons may be prescribed by law or regulation, but a notice should generally include the following information:

    - Description of what happened.
    - Type of protected data involved.
    - Actions to protect data from further unauthorized access.
    - What the Society will do to assist affected persons.
    - What affected persons can do to assist themselves.
    - Contact information for the Society's point person on data breach.

5. Actions to take following a data breach:

    - Implement remediation measures provided in notice such as credit report monitoring service to affected persons.
    - Conduct full analysis of breach to determine root cause.
    - Assess Society's internal and external controls to determine necessary changes to data collection, retention, storage and processing policies and procedures.