INDUSTRY DEFINITIONS

Security Breach and Cyber Fraud

Developed by

The SPARK Institute, Inc.
SHAPING AMERICA'S RETIREMENT

Release 1.0

April 2, 2019

The SPARK Institute, through the work of its Data Security Oversight Board ("DSOB"), developed the following definitions for Security Breach and Cyber Fraud as a standard for the recordkeeping industry in the absence of commonly accepted industry definitions.

Clients and prospects have legitimate concerns around the protection of their data and want to be informed of events that impact the security of their data. SPARK's purpose for creating this new Best Practice is to accommodate the needs of clients and prospects along with those of record keepers. These definitions are not intended to supersede state and/or federal laws, legislation, or regulation, but are meant to establish a base of communication between record keepers and plan sponsors regarding Security Breaches and Cyber Fraud events. Using these terms, clients can more accurately assess a recordkeeper's cybersecurity incident practices and controls, and use these definitions to obtain mutually agreed upon contractual protections with a recordkeeper should such an event occur.

Industry Best Practice for Defining a Security Breach and Cyber Fraud

The Spark Institute, through the work of its Data Security Oversight Board, developed the following definitions for Security Breach and Cyber Fraud as a standard for the recordkeeping industry[1]:

Security Breach is a confirmed compromise of an information system within the authority or responsibility of the recordkeeper that results in: (i) the unauthorized acquisition, disclosure, modification or use of unencrypted personal data[2], or encrypted personal data where the encryption key has also been compromised; and (ii) a likely risk of identity theft or fraud against the data subject. A good faith but unauthorized or unintentional acquisition, disclosure, modification or use of personal data by an employee or contractor of the recordkeeper or a party who has signed a confidentiality agreement with the recordkeeper does not constitute a Security Breach if the personal data is not subject to further unauthorized acquisition, disclosure, loss, modification, or use.

For illustrative purposes, examples of a Security Breach include:

- A successful attack on a recordkeeper's network or information system which results in unauthorized acquisition of participant records.
- An intrusion into a recordkeeper's external cloud account that results in the attacker acquiring unencrypted personal data stored within the environment.
- A loss of an unencrypted laptop that stores personal data where there is reasonable basis to believe that the loss may result in identity theft or fraud against the data subject.
- A data file provided to a third party who has not signed a data confidentiality agreement with the recordkeeper and where there is reasonable basis to believe that the loss may result in identity theft or fraud against the data subject.

Cyber Fraud is a confirmed compromise of a participant's financial account by a fraudster using information within the fraudster's possession or control that results in wrongful financial or personal gain or illegal access to a financial account.[3]

For illustrative purposes, examples of Cyber Fraud include:

- A participant discloses their account username and password via a phishing email link. Those credentials are then used to compromise the participant's online account and withdraw money from the account.
- A participant's computer is compromised with a form of keystroke logging malware, which captures the participant's credentials and results in the compromise of the participant's online account.

[1] Please note that these definitions serve as guidelines and do not supersede state and/or federal laws, legislation, or regulation.

[2] The term "personal data" shall be defined in accordance with the security breach law of the state of the affected individual(s), which generally includes personal information that can be used to commit identity theft.

[3] Cyber Fraud is not considered a Security Breach, unless the incident extends to a compromise of the recordkeeper's system, as noted above in the definition of a Security Breach.

- An attacker successfully takes over a participant's account and changes other participant information and/or attempts to transfer money.
- An attacker successfully gains access to a participant's account through the compromise of a third-party account aggregation technology.
- An attacker gains access to a participant's account by successfully impersonating the participant via the recordkeeper's call center.