Industry Best Practice Fraud Controls

Release 1.0
July 21, 2021

The Spark Institute, through the work of its Data Security Oversight Board, developed the following standards to establish reasonable controls to protect retirement accounts from fraud. These controls should be implemented in partnership between plan sponsors/fiduciaries, participants, and service providers (recordkeepers). These standards are not intended to provide a recommended level of fraud protection or guarantee against participants fraud losses.

In recent years there has been an increased threat of account take-overs and fraud from retirement accounts as criminals are actively targeting retirement savings. To protect these accounts there needs to be more awareness of this threat as well as sufficient controls to protect retirement assets.

A few high-profile cases over the last couple of years have highlighted this concern around fraud in our retirement system. The Government Accountability Office (GAO) and The Department of Labor (DoL) have both investigated this issue and the DoL has published cyber tips to respond to this. The need for industry recommendations and guidelines is critical to protect retirement assets. These Retirement Industry Best Practices build on the DoL cyber tips and provide more explicit recommendations to defeat retirement account fraud.

The protection of retirement accounts can only be fully realized with a partnership between Plan Sponsors, Fiduciaries, Recordkeepers, Participants and where applicable Advisors. Plan Sponsors are responsible for the overall security of these accounts. Recordkeepers must implement controls that reasonably protect, detect, and respond to fraudulent activity. Participants must act to use secure login credentials and monitor their accounts. It is imperative that there are layered controls as there is not a single solution to protect accounts. These controls should be a combination of preventative, detective, and responsive controls.

The fraud controls chart is intended to highlight a minimum set of controls that should be considered and set expectations for all parties involved.

	Control Objective	Plan Sponsor	Participant	Recordkeeper
1	**Authentication**	Plan sponsors should require that recordkeepers provide multiple authentication options.	When available, participants should enable Two Factor Authentication and/or setup additional authenticators, and should not share their login credentials	Recordkeepers should provide Two-Factor authentication for accessing participant accounts.
2	**Establishing Account Access**	Plan Sponsors should provide information to assist recordkeepers in establishing digital account access.	Participants should establish online access and set up unique login credentials (userid and password) that are not shared when they participate in a plan.	Recordkeepers should verify participant identities during account registration. Verification must involve controls beyond relying on publicly available information.
3	**Re-Establishing Account Access**	Plan sponsors should review recordkeeper controls for re-establishing account access.	Participants should establish unique login credentials that are not shared.	Recordkeepers should verify participant identities during credential reset. Verification must involve controls beyond relying on publicly available information.
4	**Contact Data**	Plan Sponsors should provide address, email, and phone numbers to enable security-related communications and Two-Factor Authentication.	Participants should ensure address, email, and phone numbers are up to date, and provide such information if not made available by the plan sponsor	Recordkeepers must seek to collect address, email, and phone from plan sponsors and participants to enable security-related communications. Preferences should be available for how emails and phone numbers are used.
5	**Communications**	Plan Sponsors should allow security related communications to be sent to participants or help distribute them internally.	Participants should review communications and statements sent from the plan sponsor or recordkeeper in a timely manner and immediately report any unauthorized activity.	Recordkeepers must notify Participants of account activity using contact data on file and should provide information on how to protect accounts.
6	**Fraud surveillance**	Plan sponsors should notify their recordkeeper if participant contact information or login credentials may have been compromised.	Participants should actively monitor their retirement accounts similar to how they monitor other financial accounts and immediately report any unauthorized activity.	Recordkeepers must have systems and processes in place to prevent, detect, and respond to potential fraud.
7	**Customer Reimbursement Policy**	Plan Sponsors should ensure a fraud reimbursement policy has been established and available to Participants.	Participants should understand their obligations within the fraud reimbursement policy for their plan and report unauthorized activity per the policy.	Recordkeepers must have a fraud reimbursement policy and should communicate it to participants.