Fraud Prevention Sub-Committee
Executive Summary

BACKGROUND	
Purpose:	The Senior Operations Council (SOC) and the Data Security Oversight Board (DSOB) of the SPARK Institute believed that the growing threats from fraud and account take-overs required an industry response. Since fraud and account take-overs involve operational processes and technical applications, the two committees created a joint sub-committee to discuss ways to address these threats. Twenty-three volunteers from sixteen member firms joined the newly created sub-committee.
Process:	The Fraud Prevention Sub-Committee held a series of conference calls to identify potential threats, examine potential solutions, and make recommendations for next steps.
Meetings:	The Fraud Prevention Sub-Committee held its first meeting August 2019 and met biweekly until January 10, 2020. During that time, members heard from outside fraud experts from FS-ISAC, LIMRA's Fraud Share Team, Early Warning Systems, PwC's Fraud Prevention Team, and the Groom Law Group.

RECOMMENDATIONS

SPARK's Fraud Prevention Sub-Committee developed a number of recommendations for the SPARK Data Security Oversight Board (DSOB) and the SPARK Senior Operations Council (SOC) to approve. These recommendations fell into three categories:

1. **Education of Plan Sponsors & Participants** – Working together plan sponsors, participants and record keepers can strengthen the system against thieves. The specific areas where our industry can help are:
    - With sponsors experiencing Business Email Compromises (BEC). Our industry can help plan sponsors better protect their email accounts
    - Assist lower-tech members of the industry, where the security chain is more vulnerable
2. **Intelligence Gathering & Sharing** – Record keepers must work across the industry to share their experiences and successes in defeating fraud. They can do this by:
    - By participating in a shared service, that allow members to disclose fraud attempts and results in a confidential way
    - There is a lot of commonality among fraud attacks, so by connecting with the larger industry community record keepers can benefit from other's experiences and even identify specific bad actors in advance.
    - A participants PII and other credentials are usually compromised in unrelated data breaches and then later used to illegally access retirement accounts. Record keepers could benefit from know if a plan or participant's PII has been previously compromised and put in place enhances security measures
    - Record keepers focus much of their attention on current activity. The industry should consider developing a means to think ahead to prevent new and different fraud attacks.
3. **Implementation of Best Practices to Prevent Fraud –** Record keepers should be encouraged to adopt the leading protections against fraud, by:
    - Participating in industry information sharing tools
    - Working to prevent attackers from first changing password and then updating email contact information before making distribution requests.
    - Implementing Multi Factor Authentication (MFA) as the necessity against fraud. Including working with telecom providers to prevent a participant's SIM card from being hijacked prior to an authentication event.
    - Preventing alerts from being misdirected
    - Engaging cross channel capabilities for both phone and web to prevent fraud