COMMENTARY

LOOK AGAIN

By Alison F. Salka, Ph.D.
Senior Vice President and Director, LIMRA Research

Building a Tower Society to Fight Fraud

People spend years saving for retirement, hoping to accumulate enough money to provide financial security for their later years. The majority of American workers cite saving for retirement as one of their top financial priorities. To that end, millions of people currently save in their employer-sponsored defined contribution (DC) plans. For about half of them, especially younger workers, this will be their primary source of retirement income.

DC plans offer the convenience of payroll deduction and are broadly available to U.S. workers. Since they are a long-term savings vehicle, some plan participants don't monitor them too closely. In addition, some plans don't send paper statements and rely on participants to log in to their accounts electronically for detailed information. While this is helpful for the environment, this is a danger for some participants. Wherever there are assets and inattention, there are also thieves.

Criminals tend to take the easiest route. DC plans have not historically been an easy target. Requiring plan sponsor approval for distributions has been a deterrent, and security processes and protocols exist to minimize fraud. Unfortunately, the vigilance of employers and service providers is matched by the determination and increasing institutionalization of fraud enterprises.

Trends in Fraud

One type of identity theft — account takeover fraud — has increased substantially. It is estimated to have grown 61 percent over the past year, totaling $2.3 billion worldwide.[1] Account takeover fraud is increasing for a number of reasons. Credit card chips have made other types of credit card fraud more difficult. (For example, losses due to counterfeit, stolen, and lost cards declined from $5.4 billion in 2016 to an estimated $2.7 billion in 2018.[2]) Those intent on fraud are now looking for new targets. New targets aren't hard to find because of private data that has been leaked or stolen in recent years. Data breaches like Equifax have become alarmingly common. Huge amounts of data have been shared and have been used to rob people of their savings. The dark web offers information about the security processes of financial services companies. This all adds up to a nightmare for both consumers and account service providers. The industry is in the crosshairs of an increasingly widespread, organized, and sophisticated criminal enterprise.

Fraud can damage a company's reputation, customer experience and loyalty, shareholder confidence, and financial results. It can be a difficult trade off; good security protocols often make it difficult to have a quick and easy customer experience. In addition, a lot of fraud is discovered by customers, not the company. When this happens, it can shake their faith in the companies they work with. Fraud can have serious financial and reputational consequences.

Not if, but When

Most financial service companies expect some degree of fraud. Credit card companies expect it, and even budget for it. They have developed sophisticated systems and algorithms to identify fraud. Other financial service providers may not be as far along. One complicating factor is that

CONTINUED ON PAGE 111

> **As fraud becomes more prevalent and costly, the industry needs to consider creating its own "tower society" for mutual benefit.**

CONTINUED FROM PAGE 112

business units often function in silos. While customers see a single brand, the reality is often a complex web of distribution channels, administrative systems, and operations that create easily exploited gaps in information. Relevant fraud information may be available to some and not others in an organization (e.g., one executive receives a report from the FBI that he is not allowed to share).

What Can We Do?

As sophisticated as our 21st century technology has become, medieval Italy may offer some lessons of value. In northern and central Italy there are a number of beautiful towers decorating towns and villages. Many of these were built around the 13th century for knights, feudal magnates, and clergy who banded together in an association or "tower society" for mutual protection. These associations grew and changed and entered into alliances with other associations. The members achieved a type of collective security. (These societies are also said to have helped build community trust and social capital that provided a foundation for democratic ideals in later centuries.)

In any case, the tower societies of Italy created a network of people who looked out for each other. Today, as fraud becomes more prevalent and costly, the industry needs to consider creating its own "tower society" for mutual benefit. If information on the latest fraud scheme is shared among companies, it will make it more difficult to perpetuate the fraud. Other companies will know what to watch out for, and can be more vigilant.

Financial services companies spend billions on security to stay ahead of criminals while still offering a good customer experience. They are committed to protecting their clients' retirement assets and financial security. Shouldn't companies support each other to help achieve that worthy goal? As the industry's trade association, LIMRA is looking into making this happen. Stay tuned for how we can help your companies combat fraud.

[1] Ben-Anchour, Sabri, "A new form of ID theft: account takeover," *Marketplace*, August 21, 2017.

[2] Karl, Sabrina, *Chip cards bring new fraud trends*, Creditcards.com, August 22, 2017.