From Fax Machines to Phishing: Why Cybersecurity Is Now a 401(k) Fiduciary Duty

By Ary Rosenbaum, Esq.

When I started back in the 401(k) business in 1998, everything was done by paper and telephone. Distribution requests were mailed or faxed. Investment changes were taken over the phone. Beneficiary designations were signed in ink and stored in filing cabinets. If someone wanted to steal retirement money, they needed forged signatures, physical access to documents, and a willingness to commit old-fashioned fraud. It was cumbersome, risky, and not easily scalable. Cybersecurity wasn't a concern, not because we were ahead of the curve, but because the curve hadn't been invented yet. It took years before TPAs even launched websites, and even longer before participants were allowed to make transactions online. Early systems were limited and slow, and most changes still required human intervention. Efficiency meant a quicker fax or a shorter hold time on the phone. The idea that participants could move substantial sums of money instantly from a mobile device would have sounded unrealistic. That slow, manual system limited exposure, even if it was inefficient.

The Digital Transformation Changed the Risk Profile

Today's retirement plan system is built on speed, convenience, and remote access. Participants expect to manage their accounts online, change investments in real time, and request distributions without speaking to anyone. Payroll providers, recordkeepers, TPAs, and custodians exchange data constantly through automated files and system integrations. What we gained in efficiency, we lost in insulation. The move to digital did not eliminate fraud; it modernized it. Retirement plans are now attractive targets because they hold large balances, operate with predictable processes, and involve multiple parties who assume someone else is double-checking the details. Cybercriminals no longer need physical access or inside help. They need credentials, and those credentials are easier to obtain than most people realize.

Cybersecurity Is a Fiduciary Responsibility

Cybersecurity is no longer an IT issue that can be delegated and forgotten. It is a fiduciary issue. The Department of Labor has made it clear that plan sponsors have a duty to prudently select and monitor service providers with respect to cybersecurity practices, just as they do with fees, investments, and overall service quality. Participant data and plan assets are plan assets, and safeguarding them is part of the fiduciary obligation. This does not mean plan sponsors must become cybersecurity experts. It does mean they must engage with the issue, ask reasonable questions, and document their decisions. Ignoring cybersecurity because it feels technical or uncomfortable is no different than ignoring investment performance because the numbers are complicated. Fiduciary duty does not disappear simply because the risk is modern.

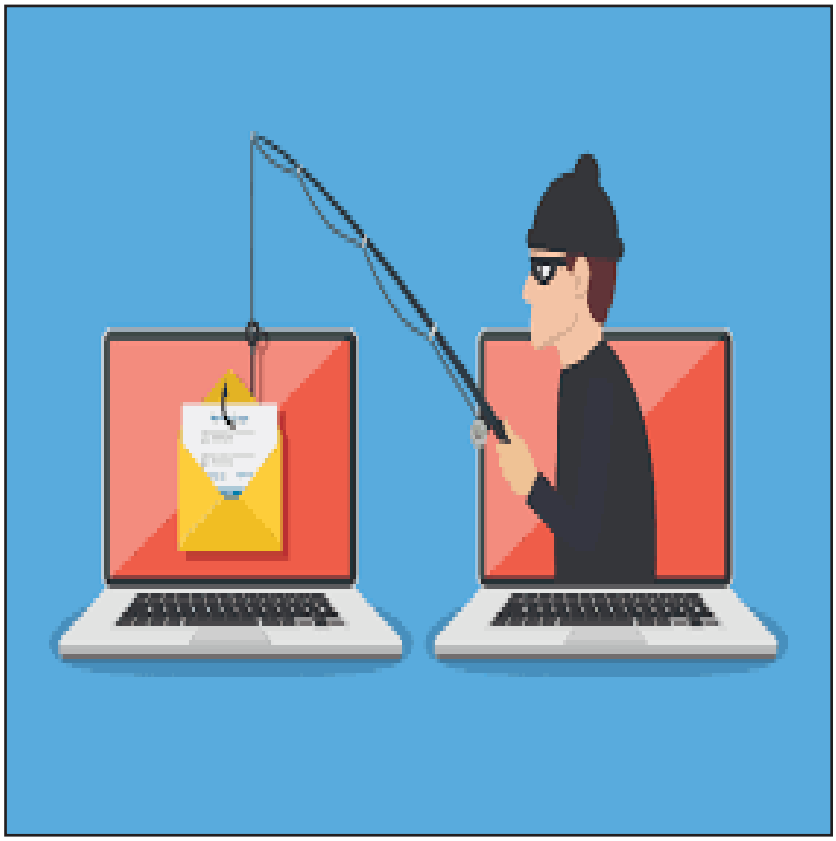
Why "That's the Recordkeeper's Problem" Fails

One of the most persistent myths in the retirement plan world is that cybersecurity is the recordkeeper's responsibility alone. While recordkeepers play a critical role in protecting participant accounts, plan sponsors are the ones who hire them, oversee them, and ultimately bear fiduciary responsibility. Participants do not sue vendors first. They sue the employer. They sue the plan sponsor whose name is on the plan document. Even the best vendor contracts do not prevent lawsuits or regulatory scrutiny. Indemnification clauses may provide reimbursement later, but they do not stop litigation from being filed or reputational damage from occurring. Plan sponsors cannot outsource fiduciary responsibility, and cybersecurity is now firmly within that responsibility.

The Evolution of Modern 401(k) Scams

Cyber fraud today is not crude or obvious. It is targeted, professional, and convincing. Account takeover fraud has become one of the most common and devastating threats to retirement plans. A criminal gains access to a participant's email account, resets the participant portal password, changes contact information, and initiates a distri-

bution or rollover. By the time the participant realizes something is wrong, the money is often gone. Phishing attacks have also evolved. Emails appear to come from recordkeepers, HR departments, or trusted vendors. Logos are accurate, language is polished, and links lead to fake portals that closely mirror legitimate websites. These scams succeed because they exploit trust, familiarity, and routine. Participants and employees are not careless; they are human.



Employers and Payroll Systems Are Targets Too

Participants are not the only targets. Employers themselves are frequent victims of cybercrime. Payroll file manipulation and business email compromise schemes can result in contributions being misdirected or stolen. An email that appears to come from an executive or long-standing vendor instructs staff to change banking information immediately. Without proper verification, funds are transferred to criminal accounts. When this happens, the consequences extend beyond financial loss. Missing contributions can trigger prohibited transaction issues, corrective contributions, and regulatory exposure. Participants want answers, regulators want documentation, and plan sponsors are left managing a crisis that began with a single fraudulent email.

Why Cyber Insurance Is No Longer Optional

Traditional ERISA fidelity bonds and fiduciary liability policies were never designed to address modern cyber risks. Many policies explicitly exclude losses caused by hacking, social engineering, or electronic fraud. Cyber insurance exists to fill that gap. A proper cyber policy can cover theft of plan assets due to cybercrime, data breach response costs, forensic investigations, legal defense expenses, notification requirements, and credit monitoring. Without cyber insurance, plan sponsors may find themselves paying for these costs out of pocket. The financial exposure can easily reach six or seven figures, particularly when participant balances are involved. In today's environment, carrying cyber insurance is no longer a luxury or a best practice; it is a necessity.

Fidelity Bonds Are Not a Cyber Safety Net

There is a dangerous assumption that fidelity bonds will automatically protect against cyber theft. Fidelity bonds are intended to protect against dishonest acts by plan officials, not sophisticated external attacks. While some policies may provide limited coverage, exclusions are common and often misunderstood. Discovering after a loss that coverage does not apply is a hard and expensive lesson. Plan sponsors should not assume coverage exists simply because a bond is in place. Understanding what is covered, what is excluded, and where cyber insurance fits into the overall risk management strategy is essential.

Engagement, Not Perfection, Is the Standard

Cybersecurity does not require perfection, but it does require engagement. Plan sponsors should understand how participant authentication works, whether multifactor authentication is mandatory, how distribution requests are verified, and how incidents are handled when something goes wrong. Providers should be able to explain their processes clearly and transparently. Participant education is also critical. Simple guidance on password security, recognizing suspicious emails, and verifying transactions can prevent many incidents. Education is inexpensive, effective, and demonstrates fiduciary prudence. Internal staff training is equally important, particularly for HR and payroll personnel who are frequent targets of fraud.

Cybersecurity Is the New Fiduciary Frontier

When I started in this business, the biggest operational risk was a lost form or a miskeyed number. Today, a single compromised login can drain a lifetime of savings in minutes. The tools have changed, but the responsibility has not. Cybersecurity is simply the next evolution of fiduciary oversight, no different in principle than monitoring fees or investments. Plan sponsors do not need to panic, but they do need to act. Asking questions, carrying appropriate insurance, educating participants and staff, and documenting decisions will not prevent every incident, but they will define how a plan sponsor is judged when something happens. And in today's digital environment, something eventually will.

The Rosenbaum Law Firm P.C.

The Rosenbaum Law Firm P.C.
734 Franklin Avenue, Suite 302
Garden City, New York 11530
(516) 594-1557

http://www.therosenbaumlawfirm.com