Identity Theft: The Rising Threat to Retirement
How You Can Make a Difference

Alison J. Cohen, Esq.

The day starts as any other. A distribution form comes in for processing. It has a participant signature. The spousal consent section is completed and notarized. The Plan Administrator has signed the form. No problem. So, you process the $450,000 in-service distribution and give it no further thought. Three days later, the real participant calls in a panic wondering where his money went. Yikes?

As a third party administrator (TPA), what can you do to help thwart this brazen, growing band of thieves? Do you have an obligation to do anything? What if your firm is acting as an ERISA 3(16) delegated fiduciary? Lot of questions, but we have no concrete guidance from any federal agency.

What a TPA Can Do with Internal Procedures

Although it would not have helped in our real-life situation described above, requiring that your clients use your secure portal to transmit data is an easy first step. It should be spelled out in the TPA's service agreement, enforced in the onboarding process, and reiterated every time the client fails to use the portal. Consideration should also be given to adding footers/disclaimers on every outgoing email to consistently remind clients of the importance of using the portal.

Discuss internally whether you can support your client by implementing additional safeguards, such as:

- Have those who process distributions review the participant contact information carefully – make sure that the phone number, email address, physical address, marital status, etc., match the TPA's and/or Recordkeeper's (RK) records;
- Contact the Plan Administrator by telephone for personal verification when the distribution requested is over a certain dollar amount;
- Consider sending an email to the participant at the known email address on file (preferably the work email, if the request is for a loan or in-service distribution) that simply acknowledges receipt of the request. If the participant didn't make the request, he or she is likely to reach out immediately and stop the process;

- Flag accounts for a reasonable period of time after the participant files an address change and scrutinize any withdrawal or loan requests that come in during that period (the address change can be the first step of the fraud by someone other than the participant); and
- Compassion is a beautiful thing, but don't fall for the applicant's pleas to break existing procedures. Criminals are good liars and procedures exist for a reason; make sure that they are followed without exception.

Big financial institutions/RKs have been moving to multi-key recognition software – such as voice recognition and secondary PINs. While the typical TPA can't afford this level of protection, you can consider partnering with RKs who have taken these steps to help protect your clients…and YOU. If you've been doing this long enough, you remember when the trend was to go totally hands-off for processing. The days of fully automated flow-through/no touch are on their way out, as participants/consumers would rather have safety instead of speed.

How TPAs Can Help Clients and Win Loyalty

Not everyone is comfortable with online portals and other technology designed for secure delivery. Provide training on the use of your firm's secure transmission methods for all client contacts. Using certain services, such as Go To Meeting or Zoom, can allow you to show the client on a shared screen, increasing his or her comfort level.

Create a Best Practices document that you provide to all of your clients and make available on your website. Recommendations you can include:

- Encourage Plan Administrators to verbally verify certain "high target" transactions;
- Encourage participants and plan sponsors to change to online statements, instead of paper copies sent via the mail. Paper documents can be intercepted, and this valuable information can be used to assist in a fraudulent distribution request;
- Create verification checklists for the Plan Administrator to use, including such questions as:
    - Has the participant submitted a change of address request in the past 3 – 4 weeks?
    - Does the address on the form match the employer's records?
    - Does the phone number on the form match the employer's records?
    - Does the email address provided match the employer's records?
    - Verify the Instruction for distribution – is the check going to an address at a location other than the participant's home or office?
    - Verify the bank account information for a wire transfer – is it in the name of the participant? Can you verify that with the bank?
    - Is the spouse's name correct?
    - Does the signature of the participant and/or spouse match prior forms submitted?
    - If the request is for a distribution or loan in excess of a certain dollar amount, has verbal confirmation been received from the participant based on contact information NOT on the form (alternate phone)?

What if Our Firm Is a 3(16) Delegated Fiduciary?

If your firm has agreed to take on the review and approval process for the distribution and/or loans in a 3(16) fiduciary capacity, the question of whether there is an obligation to take any of these steps is moot. As a fiduciary, you ARE responsible for the outcome of this transaction. That means that you should have extra steps and procedures in place to ensure that the funds approved to be distributed are going to the actual participant. So, all of the above steps and suggestions should be considered and implemented to the extent possible.

Other Considerations

TPAs should have a discussion with their E&O insurance carriers to see whether the policy would cover a case of identity theft (even if the TPA is incorrectly accused of being responsible). Many (and, these days, it should be *all*) TPAs also have cybersecurity insurance; however, those policies may only cover theft via cyberattack, such as hacking. Cybersecurity and identity theft are two sides of the same coin, but they are not necessarily covered the same way in the policy. It is certainly worth asking the question before it's not hypothetical.

Once a theft has been reported by a participant or plan sponsor, you should have procedures in place so that everyone knows what to do next. For example, you need to have a list of phone numbers to immediately contact the major banks, the custodians, FBI, etc., so that there is a chance of quick recovery after the event.

In the scenario we started with, the TPA quickly contacted the custodian and tried to get them to recall the wire. They also finally found the right number at the receiving bank for its fraud department to try to get cooperation from that end. Unfortunately, by the time the receiving bank was notified, the funds had been transferred out of the account by the thief. The FBI was brought in, but, by then, more than a week had passed after the distribution was made. The tax withholding was able to be reversed and returned to the participant. The plan sponsor is still determining how to make the participant whole.

Conclusion

"Be vigilant and be prepared" should be a TPA's motto when it comes to money leaving the plan. Consider what the amount is that could be replaced at your expense if you were held responsible for a theft, and make sure that your procedures and cross-checks ramp up to a high level once the distribution or loan exceeds that amount. It's much, much better to be safe than sorry.

FERENCZY
BENEFITS LAW CENTER
We are your ERISA solution™

Ilene Ferenczy • ilene@ferenczylaw.com | Alison Cohen • acohen@ferenczylaw.com
Adrienne Moore • amoore@ferenczylaw.com | Adriana Starr • astarr@ferenczylaw.com
Tia Thornton • tthornton@ferenczylaw.com | Leah Dean • ldean@ferenczylaw.com

2635 Century Parkway Suite 200, Atlanta, GA 30345
T 404.320.1100 | F 404.320.1105 | www.ferenczylaw.com