July 14 Webinar – Get Your Hands Off My Money! – Alison, Adrienne, Adriana

1. Even if they had asked where do you live, the thief could have given a different address and said whatever they had on file was old, correct? Barnett v Abbott
   This is why you need procedures in place related to address changes. If you allow someone to change their address at the time they are requesting the distribution, you need additional assurances that the address they are giving is valid. We often recommend administrators require any address changes come through the Plan Sponsor or be accompanied by a Medallion Signature Guarantee. Another best practice is to delay distribution or loan requests after a change of address until the participant can receive a confirmation of the change and object, as necessary.
2. Hi, a somewhat obvious question...if the funds are transferred, wouldn't there be more of a chance to find who is stealing the money? Leventhal Case
   Sadly, this is not often the case. The fraudsters generally already have enough information to create fake identification and set up an account often in the name of the participant. By the time you've chased them down, they've transferred the funds out to an offshore account, closed the fake account, and the money is gone.
3. Where should the emails be saved? Case Study 2 – Adrienne
   I assume this in reference to our statements throughout the webinar indicating that it was not ideal to (1) use personal email or (2) keep an abundant number of emails in your inbox/sent folder/trash. In MandMarblestone specifically, the TPA has alleged that the use of a personal email address by an employee of the Plan Sponsor caused the breach to occur because it is believed this personal account is where the breach occurred. Generally, the expectation is that a personal email address will be less secure than your work email. Many factors relate to this. For example, your employer (hopefully) invests more in security than you do personally, you are more on guard when reviewing work emails, your employer likely sets up and updates its email filters regularly, etc.

   Beyond this, we recommend not keeping all emails in your mailbox in perpetuity. The alternative is to save and store your emails in another document retention program that is in the Cloud or some other secured server that's not so easily accessible. (By way of example and not necessarily as an endorsement, our firm currently uses Worldox.) By using a separate program, all emails are stored in a separate secure program. We also delete older emails so that if anyone gained access to our mailboxes, they would only have a few months of data (potentially still substantial!) as opposed to our entire history, which is stored outside of Outlook.
4. Does Cyber coverage always cover the loss of actual plan assets? We know it covers forensic research, cost of notifications, etc. but not so sure it covers third party asset losses.
   It depends on your coverage. Many policies do not cover the loss of plan assets. You should review your policy carefully to be certain.
5. I thought it was OK to open any email, and that the only dangerous action would be clicking on a link in the email.

To our knowledge (and as was the case in all of our firm's case studies), breaches occur when a person receives an email and unwittingly clicks on a link or opens an attachment that gives a third-party fraudster access to the account. No promises on the abilities of criminals in the future.

6. We use G-mail for work... you can archive your inbox but would that really do anything? Would seem we should really archive outside of G-mail?
   To our knowledge, the archive function within Gmail only removes an email from your inbox and does not provide additional security. It can still be accessed if the account is breached. You should determine with your IT department how to save emails outside of Gmail.
7. What criteria should be used by a TPA to approve a daily record keeper online distribution request?
   The benefit of online distribution requests is that you can have automatic processes to kick up red flags. Possible items to require greater scrutiny would be: a participant changes his/her password within the past 30 days, the participant changed his/her address within the past 30 days, the participant took a distribution within the past 30 days, the distribution exceeds $X (determine your risk tolerance) or is a total distribution of the account, etc. With online requests, it's also best to have multifactor authentication and immediate notices. Any change to the account or request should trigger a confirmation email to the participant (and, consistent with the above recommendations, that should go to an email address that has been in place for at least 30 days). There really are many options and you'll have to weigh what level of risk you're willing to take versus how much additional scrutiny you can reasonably provide. If anyone wants to discuss specifics in greater detail, please feel free to reach out to one of us.

8. Do you see any current trends that fraudsters are using to either Socially Engineer or gain access to participants accounts/personal data?

   Alison – With the pandemic, there are many sad stories out there that can tug at one's heart strings. In an effort to be helpful and customer service oriented, TPAs are unwittingly giving too much information away. We have talked to one TPA that had the same fraudster try calling multiple times thinking they were going to get different people. But, as a small vendor, it was the same staff member and she recognized the voice immediately. Stick to your procedures.

   Adrienne – Spoofed email accounts. And they are getting harder to spot. We've seen ones that appear to be a genuine email and the only change has been a capital I to a lowercase L, or two letters are inverted. The eye very easily does not pick up on this. Without the red flags of misspellings and grammar we're more used to seeing, these can be difficult to spot, and a lot of information can be turned over to someone who appears genuine.

   Adriana – Fraudsters will attempt to login using information they already have. For example, the fraudster may have the participant's date of birth and Social Security Number already. The fraudster will attempt to change the password and if they are lucky enough will be able to avoid the security questions like the fraudster in Abbott. This man took the scam one step farther by intercepting the participant's mail to prevent the notification of disbursement from reaching

them. https://www.justice.gov/usao-cdca/pr/orange-county-man-indicted-charges-he-stole-boeing-employees-identities-siphoned-money

9. I like to save emails in client folders in my email that I can refer to as proof of conversations and reference if I can't remember a conversation. I'm seeing this is probably a bad choice. Should I only be concerned with emails that contain personal information or should I be deleting all emails regularly. I like to have saved emails especially when a client says, "I never got that" and I can go back and forward my original email to them.

   It is safer to delete all of your emails regularly as a belt and suspenders approach. If you only delete emails with personal information you may end up missing one and your efforts will be all for naught. Email archiving is your friend! Software is available to not only archive, but to organize prior communications with clients. You should be able to access that email your client "never got" without having to rely on your inbox. I believe some of the TPA specific secure portals offer email tracking that provide proof of delivery. We recommend working with IT professionals to establish policies and put software in place to ensure that your data is safe.

10. Does the cyber security insurance policy have to be for the TPA only? Our company has other employer service divisions, such as HR and payroll.

    It depends upon the insurer and your organizational structure. You should discuss your policy with your insurer and ask pointed questions. It is important to understand what the policy does and does not cover. Which divisions are covered? What is a covered data breach?

11. Great timing....just got this call today. Participant called in and said he got a quarterly statement from one of our plans he has never worked for/heard of. Long story short - the account has $3k in it from an employee who stole his identity in 2001 and he's been fighting identity fraud ever since he found out in 2004. The bad actor termed 3 years ago. The victim doesn't want the money, he just wants the communication to stop. What does the TPA/Record keeper do in this case? Assets in the account can't be forfeited back to the plan at this time even in the case of fraud. What should we do?

    The Plan Sponsor is the one on the hook for not properly vetting its employee and should be made to address the situation. The TPA/RK should not be taking on the legal liability for making the decision on what to do with the funds. The victim should provide the information to law enforcement so they can try to locate the thief. The Plan Sponsor's legal counsel may direct them to move the funds to forfeiture regardless.

12. How about the Sent Folder? Delete over 30 days?

    The sent folder is just as much of a threat as the deleted folder. Deleting and archiving sent emails over 30 days is a great policy.

13. Wouldn't a check shift the responsibility to the depository bank? If they accept the deposit, they have the responsibility to make sure the endorsement is valid. (Bank wire transfer held, then released)

    The benefits of distribution by a check means there is likely a few days delay between the check being received and it actually clearing in the receiving bank. As far as liability, banks are supposed to only open accounts after verifying the actual identity of the individual opening the account. It's a legal requirement, but we know that they fail to do this all the time. No one has yet to file suit against the banks with the fraudulent accounts, to our knowledge. Proving their negligence would be an interesting challenge.

14. I have had two plans provide me with their login and passwords for their prior TPA accounts. One of them even provided me answers to security questions! I advised them to change their passwords (and security questions) immediately. What else would you recommend?

    Sharing logins is a dangerous business, even internally. You do not want to be responsible for the security of your client's information. Never agree to accept such confidential information for your own protection. You should require your clients to complete the necessary paperwork for you to have your own login.

15. Would you recommend TPA offer "3(16)" services to help alleviate some burden off the plan sponsor especially with distributions" Or would you consider it not worth it?

    The answer depends upon the TPAs cost benefit analysis. We can discuss the risks and rewards of offering 3(16) services, but at the end of the day it is the TPA's business decision. What we will say to any TPA that is considering offering 3(16) services needs to have fully detailed procedures, proper oversight, an iron-clad service agreement, and proper insurance.

16. Regarding Mr. Owen's original question above, regarding having access to emails within any folder within the email system: we send & receive emails "securely" using a third-party service to encrypt the emails containing personal information; are these emails, though sent & received securely, similarly visible if a phisher successfully accesses an email account?

    It depends on the set up of your third-party service. If you can access an unencrypted census sitting in your sent box it is likely that a phisher can access the information as well. You should reach out to the third-party service's customer service or consult with an IT specialist.

17. What sort of information should you delete from social media?

    The danger of social media is providing fraudsters with information that may reveal answers to security questions associated with your logins. I recommend answering your work security questions with inaccurate responses. For example, if the security question is "What elementary school did you attend?" the answer should not include the name of the elementary school you actually attended. This prevents fraudsters from scrounging together enough information from your social media to answer your security questions. Don't put your address and date of birth on blast on social media either. Don't use any birthdays, pet's names, kid's names, etc. as passwords. There are many suggestions on how to protect yourself and your information. One

of the first and best things you can do for yourself instantly is to freeze your credit with all three major credit monitoring services. It's free and takes about 15 minutes.