GEMMER ASSET MANAGEMENT LLC
LOCAL PARTNER GLOBAL INVESTING

Advisor Connect

Operations Newsletter

Issue Number 8 Date 06/30/2017

Importance of Updating Beneficiary Information

Everyone knows that updating beneficiary information is important. All too often clients commit costly mistakes that may leave loved ones out in the cold despite their best intentions.

For instance let's say a client has three children: Abe, Bella, and Charlie. Abe has two children – their grandchildren. The client names all three children as beneficiaries on their IRA, intending each to inherit one-third of it. If Abe predeceases the client, then when the client dies Bella and Charlie will each receive 50% of the IRA, instead of the one-third – while the grandchildren by Abe will receive nothing.

This was a real life situation that actually happened when a client failed to update their beneficiary information and accidentally disinherited their grandchildren. This is a prime example of why it is so important to make sure beneficiary information is up to date. We know each advisor wants to do right by their client and their family members. Gemmer performs an IRA beneficiary update project every three years to make sure IRA beneficiary information is up to date. This year, in 2017, we are due for another update, so we will reach out to your office in the 3rd quarter to discuss in greater detail.

How does Per Stirpes or Per Capita work?

One of the most common questions that we receive is "how does per stirpes or per capita work?". To understand how per stirpes or per capita work in different scenarios, attached is an illustration of some examples. At this time, clients cannot use "per stirpes" or "per capita" designations on the Schwab Account Application and must sign the custodian's IRA Beneficiary Update form to use these designations. Schwab has recently updated their beneficiary designation form to include per stirpes and per capita as available options. For Fidelity and TD Ameritrade accounts, the process is a bit different. Please contact us if you would like to learn more.

Required Minimum Distribution (RMD) Aggregation Rules

As your clients age, more and more will be reaching the RMD age of 70½ . With so many clients needing to take different amounts from different accounts, it can be hard to remember the rules and some clients would like to take their RMD from as few accounts as possible. To make sure your clients do not suffer from the possible 50% penalty for a missed or short RMD, below is an aggregation rules chart.

Type of Account	RMD Aggregation Rules
IRAs	RMD for each IRA account to be calculated separately but the total can be taken from one or more of those IRA accounts
Roth IRAs	There are no RMDs for Roth accounts
Inherited IRAs (all types)	RMD must be calculated and taken separately for each account
Company Plans	RMD must be calculated and taken separately for each account
403(b) Plans	RMD for each 403(b) account to be calculated separately but the total can be taken from one or more of those 403(b) accounts

Educate Your Clients About Cyber Security

By now we hope your firm has established a protocol for protecting your clients. Now it's time to help them protect themselves.

We've attached a Cyber Security Toolkit which includes the following:

- Six ways clients can help protect themselves.
- Communication plan for existing and new clients.
- Sample client letter.
- Common tactics used to steal identity and login credentials.
- Investor Protection Checklist.

Training Videos

Remember that Gemmer has training videos on the website under Advisor > Tools. If you need any help logging in, please contact the Gemmer operations team.

Stay Tuned Section:

Gemmer will be contacting advisors about their clients needing to take their 2017 RMDs in the 3rd quarter. In addition, we ask advisors to calculate the RMDs for Inherited IRAs.

Beneficiary Designations “Per Stirpes” and “Per Capita”

What is “Per Stirpes” and “Per Capita”?
Per stirpes (which is Latin for "per branch") specifies that each branch of the deceased person's family receives an equal share of the estate, regardless of how many people are in that branch.

Per capita means “by total head account” or “by total number of individuals”. It means that all the living members will receive an equal share.

How are they different?
Per stirpes is different from per capita, because per capita weighs each person equally, rather than each branch equally.

Which is used more often?
Per stirpes is used more commonly in estate planning than per capita because it covers the typical family situation.

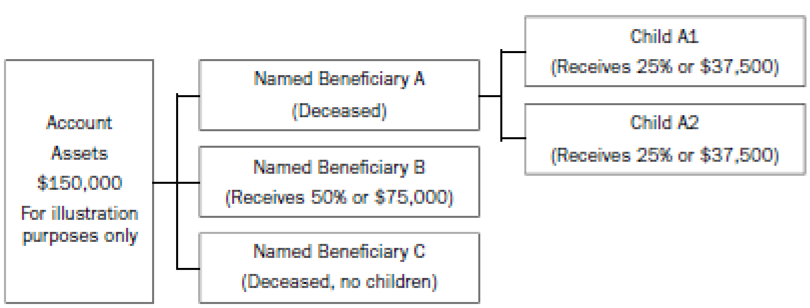
Are there other considerations?
If your client prefers to use a per capita distribution, then they will need to make sure that the estate plan addresses any generation-skipping shares that may be created by this type of distribution.

When using the “per stirpes” or “per capita” designation, the term “children” refers to natural or legally adopted children; stepchildren are not legally defined as children for this purpose.

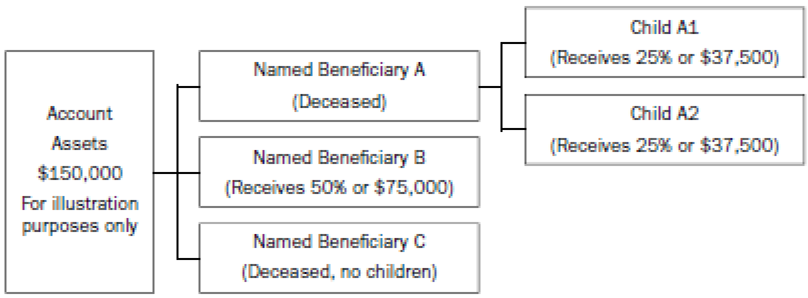
Here are some illustrations:

Example 1: There is Beneficiary A, B, and C. Beneficiary A is deceased with children. Beneficiary B is still living. Beneficiary C is deceased with no children.

Example 1A – Per Stirpes



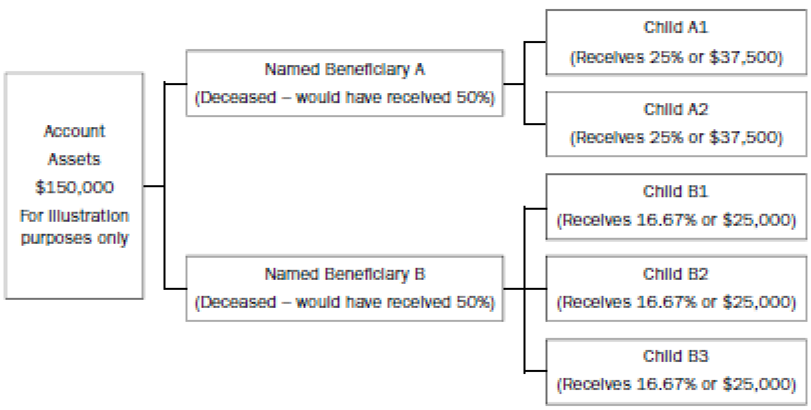
Example 1B – Per Capita



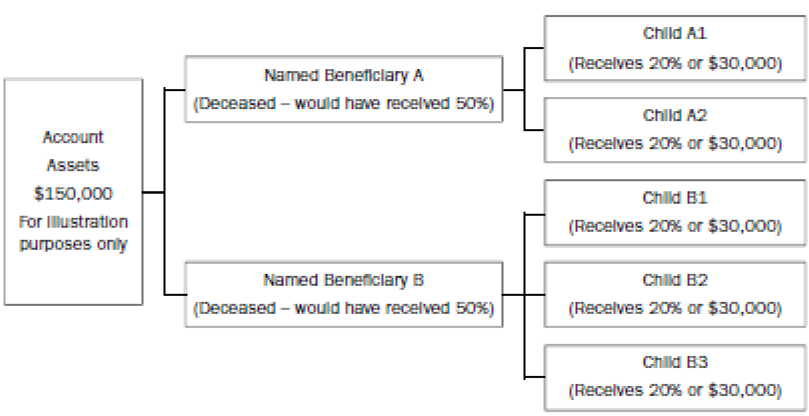
The end result is the same under both per stirpes and per capita distribution.

Example 2: There is Beneficiary A and B. Both beneficiaries are deceased and each had children.

Example 2A – Per Stirpes



Example 2B – Per Capita



The end results are different based on whether you selected per stirpes or per capita distribution option.

If you have any questions, please contact a member of the Gemmer Operations team.

Client Toolkit
Cybersecurity Best Practices

You may be protecting your client from cyber fraud, but what are THEY doing to protect themselves? We hope the resources in our toolkit help arm your clients against fraudsters!

Six Ways Clients Can Protect Themselves

Cyber Fraud Client Communication Plan

Recommendations for All Clients

- Send customized copies of the attached client letter and protection checklist to all clients.

- Determine which clients may benefit from a follow up phone call to discuss in more detail.

- During your annual client meetings, discuss the importance of protecting themselves again fraudsters. Provide them with copies of the protection checklist and share any new best practices you've learned since your last meeting.

Recommendations for New Clients

- Discuss the importance of protecting themselves against cyber fraud. Share a story that may help them understand it's not if, but when they may have a run in with a fraudster. Give them a copy of the client letter and protection checklist.

- Tell them about your procedure for protecting their personal information. They need to know you are doing your part as well!

Sample Client Letter

Dear Client:

Keeping your information secure from criminals is a top priority for our firm. To better protect you and your accounts from cybersecurity threats, we continuously review security procedures to ensure that we are following best practices recommended by the custodians, financial institutions and industry experts with whom we work.

While we feel we are taking clear and actionable steps in our own firm's security measures, cyber fraud continues to escalate, is becoming more sophisticated and is ever changing. These threats take various forms, including email scams (e.g., phishing), where criminals obtain investors' identity and use that information to commit various forms of wire fraud. The attachment to this letter describes these phishing scams and other tactics that we believe investors should be aware of.

As a fiduciary to your financial accounts, we are encouraging our clients to embrace a series of measures to help protect their identity and mitigate potential security risks. The attached investor protection checklist outlines some best practices for investors across six key areas to help you:

- Manage your devices
- Protect all passwords
- Surf the Web safely
- Protect information on social networks
- Protect your email accounts
- Safeguard your financial accounts

Please carefully review this checklist with all members of your household. We also ask that you do the following:

If you change a current address, notify us so we can update our records.
If you suspect that your email account has been compromised, call us immediately.
If you suspect that any of your investment accounts have been compromised, call us immediately. If it's after hours, contact the custodian directly and ask for their fraud protection team to inform them of suspicious account activity.

Do not hesitate to contact us with any questions or concerns about how we protect your accounts or the steps you and your family can take to better protect yourselves and mitigate risk. As always, we appreciate the opportunity to help you achieve your financial goals.

Sincerely,
(Insert your name here)

Attachment: Common tactics used to steal identity and login credentials

Some of the most common tactics criminals use to compromise a victim's identity or login credentials are described below. After gaining access to an investor's personal information, criminals can use it to commit various types of fraudulent activity. The action items presented in the investor protection checklist are intended to help you and your family better protect yourselves against such activity.

- **Malware:** Using malicious software (hence, the prefix "mal" in malware), criminals gain access to private computer systems (e.g., home computer) and gather sensitive personal information such as Social Security numbers, account numbers, passwords, and more.
  How it works: While malware can be inserted into a victim's computer by various means, it often slips in when an unwary user clicks an unfamiliar link or opens an infected email.

- **Phishing:** In this ruse, the criminals attempt to acquire sensitive personal information via email. Phishing is one of the most common tactics observed in the financial services industry.
  How it works: Masquerading as an entity with which the victim already has a financial relationship (e.g., a bank, credit card company, brokerage company, or other financial services firm), the criminals solicit sensitive personal data from unwitting recipients.

- **Social engineering:** Via social media and other electronic media, criminals gain the trust of victims over time, manipulating them into divulging confidential information.
  How it works: Typically, these scammers leverage something they know about the person - like their address or phone number – to gain their confidence and get them to provide more personal information, which can be used to assist the criminal in committing fraud. Social engineering has increased dramatically, and many times fraudsters are contacting investors by telephone.

Investor Protection Checklist

The educational checklist presented below is designed to help you take appropriate actions to better protect you and your family and mitigate risk of cyber fraud. Carefully review the items in each of the categories below to determine which apply to your unique situation.

Topical Area	**Actions to Consider**	**Check when Completed**
Manage your devices	• Install the most up-to-date antivirus and antispyware programs on all devices (PCs, laptops, tablets, smartphones) and update these software programs as they become available. These programs are most effective when users set them to run regularly rather than just running periodic scams, which may not provide maximum protection to your device. • Access sensitive data only through a secure location or device; never access confidential personal data via a public computer, such as in a hotel or cybercafé. • If you have children, set up a separate computer they can use for games and other online activities.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect all passwords	• Use a personalized custom identifier for financial accounts you access online. Never use your Social Security number in any part of your login activity. • Regularly reset your passwords, including those for your email accounts. Avoid using common passwords across a range of financial relationships. • Avoid storing passwords in email folders. Consider using a password manager program.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Surf the Web safely	• Do not connect to the Internet via unsecured or unknown wireless networks, such as those in public locations like hotels or cybercafés. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect information on social networks	• Limit the amount of personal information you post on social networking sites. Never post your Social Security number (even the last four digits). Consider keeping your birthdate, home address, and home phone number confidential. We also discourage clients from posting announcements about births, children's birthdays or loss of loved ones. Sharing too much information can make you susceptible to fraudsters and allow them to quickly pass a variety of tests related to the authentication of your personal information. Never underestimate the public sources that individuals will use to learn critical facts about people.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Protect your	• Delete any emails that include detailed financial	☐ I've reviewed and

email accounts	information beyond the time it's needed. In addition, continuously assess whether you even need to store any personal and financial information in an email account. • Use secure data storage programs to archive critical data and documents. • Review unsolicited emails carefully. Never click links in unsolicited emails or in pop-up ads, especially those that warn that your computer is infected with a virus and request that you take immediate action. • Establish separate email accounts for personal correspondence and financial transactions.	understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.
Safeguard your financial accounts	• Review all your credit card and financial statements as soon as they arrive or become available online. If any transaction looks suspicious, immediately contact the financial institution where the account is held. • Never send account information or personally identifiable information over email, chat, or any other unsecure channel. • Suspiciously review any unsolicited email requesting personal information. Further, never respond to an information request by clicking a link in an email. Instead, type the Web site's URL into the browser yourself. • Avoid developing any online patterns of money movement, such as wires, that cyber criminals could replicate to make money movement patterns appear more legitimate.	☐ I've reviewed and understand all the items in this topical area. ☐ I've taken action for those that apply to my situation.