

MSBA PROBATE & TRUST LAW SECTION E-NEWSLETTER

April 2017

Call for Submissions

We are always looking for attorneys to write brief articles for this newsletter. Articles can focus on any issues relevant to probate and trust law. This newsletter is distributed to the Probate and Trust Law Section membership, which consists of approximately 1,107 practitioners. Writing for the newsletter is a great way to share your knowledge and expertise with your colleagues.

If you are interested in submitting an article, please contact Jess Geisler (jess@geislerlaw.com) or Emma Maddy (emma.maddy@stinson.com) with your idea.

Please visit the Section's website for ideas and to see the various articles that have been written in the past.

Best Regards,
Probate & Trust Newsletter Editors

Seeking Mentors

The Probate and Trust Law Section's new mentoring program is looking for attorneys who would be willing to serve as mentors of mentees living in the following communities:

Albert Lea, Tyler, North Branch, and Delano.

The mentors do not necessarily have to be from those communities. If you are interested or have questions, please contact Touch Thouk at touch.thouk@stinson.com.

Upcoming Events and CLE Programs

- **Greater MN Probate & Trust Study Group Conference Call**
 - Wednesday, April 19, 2017 at 9 a.m. (the 3rd Wednesday of every month)
 - Call-in Number: (800) 406-9170 passcode: 1491722
 - Contact JoEllen Doebbert (320-763-7838) with any questions or to join the group.

- **MSBA Probate & Trust Law Section Meeting**
 - April 20, 2017 at 3:30pm
 - Location: MSBA Office in City Center, Minneapolis

- Please keep an eye out for additional information on the [2017 Probate & Trust Law Section Conference](#)- June 12 and 13 at the RiverCentre in St. Paul.

Case Law Update

There are no cases to report this month.

Federal & Minnesota State Tax Update

No report.

Tech Tip

Password Management 101

Richard Baum, Chair, Technology Committee, Probate and Trust Section

For decades the daily checklist went something like this: wallet, keys, cell phone, and where do I need to be today. Thanks to technology another item to add to this list is what passwords do I need. In addition to keeping our passwords accessible and secure, we must ensure they are strong. This brief article is designed to start a conversation about how you can keep your passwords secure and strong.

What can be done?

Password managers can alleviate a lot of the aggravation of recalling passwords and keeping them secure. Some will also allow for password management after your death to assist with winding up your digital life.

What are your choices?

There are a lot of options for password managers. Some store information on your computer while others utilize cloud storage. It pays to do your due diligence so you feel comfortable with the choice you make. Here are four options you can consider (there may be others) and some pros/cons for them:

- **Old school or 21st century.** Old school password managers are pencil and paper. You write them down in a book and keep the book physically secure (not a post-it note on your computer or desk). You write them in pencil because you may need to change them and it is easier to erase than scratch them out to write a new one. You must also have a trusted person know where those passwords are stored in the event you are gone. The 21st century route is a password manager service. A good service will be secure, allow you to store a large number of passwords and will suggest strong passwords for you. Even better ones will tell you when a password is not strong. You will be at the mercy of that service, so it better be available well into the future. Finally, you must have a password to access that service. That means you may have to remember one password that is outside of the password manager service, but hey, at least it is only one password.
- **Free or paid service.** “You get what you pay for” can be true here. If you want to go the free route, you may have a limit on the number of passwords that can be stored/managed

or the number of features that are available. Paid services typically offer more features, and presumably have stronger support. PC Magazine does annual reviews of free and paid password managers; search “password manager reviews” and insert “free” or “paid” to narrow down to either category. A password manager service also may offer a “legacy” option where your personal representative can have access to your passwords to be able to shut down accounts.

- **Browser-specific.** If you are dedicated to one browser that is not Internet Explorer 11, then Firefox and Chrome both offer password manager features, and both claim to be secure. Searching for “Chrome password manager” or “Firefox password manager” to read more about their capabilities. Why the knock on Internet Explorer? Well, Internet Explorer is a hacker’s dream because so many people use it, and many fail to take steps to ensure it is up to date. Knowing that you have a large, captive audience ensures you can devote resources to attack that vulnerable segment. Chrome and Firefox, while not perfect, are arguably better designed to look out for and respond quickly to bad stuff better than IE. What about Edge? Read the next bullet.
- **Operating-specific or not.** If you relish reading about the PC versus Apple debate, the next few sentences are for you. Apple products come with their own password manager called Keychain. Assuming you create an Apple ID and link all your Apple devices together, your passwords should flow from one device to another. Having passwords saved across devices will only work if 1) you use Safari as a browser and 2) Keychain decides to work for you. I am an Apple user and can attest to the sometimes inconsistent application of passwords across devices. Another mild annoyance with Keychain is that password management is not the same on iOS devices versus desktop Macs. Microsoft Edge (the replacement for IE) supposedly has a password manager, but an internet search on that subject returns articles that are 12-18 months old, and no one seems to be writing glowing reports about it. If you are a PC user, I suggest you either rely solely on Firefox and Chrome, or go the dedicated password manager service route.

One additional tip

Winding up digital accounts will become more important as time goes by, and Minnesota now has the ability (through chapter 521A) to designate a fiduciary to manage your digital assets once you are gone. Be sure your estate planning documents include granting your fiduciaries access to digital assets (including electronic communication).

Your takeaways:

1. Use some sort of password manager
2. Use strong passwords
3. Designate someone as your digital account contact, in your estate planning documents and within your password management system if you choose to use one (and it has that option)

Newsletter Committee Co-Chairs: Emma Maddy and Jessica Geisler

To access the PROBATE & TRUST LAW SECTION WEBSITE |Click [here](#)

If you do not wish to receive this E-Newsletter, send your request to be removed from the mailing list to Tram Nguyen at tnguyen@statebar.gen.mn.us.

Current and prior E-Newsletters are posted on the website for the MSBA Probate & Trust Law Section and are available at: [Probate & Trust Law Section Newsletters](#)