Protecting Digital Property

Ten NEW Challenges - Ten NEW Planning Opportunities

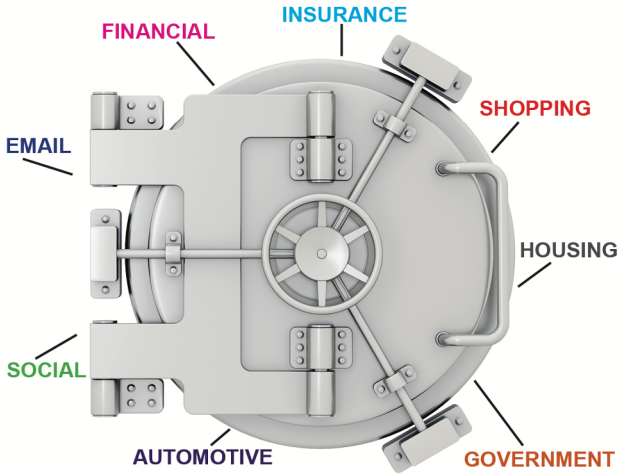
Betsy L. Ehrenberg
CEO, Legacy Concierge
betsy@legacy-concierge.com

Digital Property is Everywhere

Most people under 65 have more than 160 different digital accounts.

Digital Property is Elusive

- Usernames and passwords
- Paperless financial accounts
- Bill pay and housing costs
- Smartphone PIN and messages
- Auto/house/life insurance
- Apps uploaded to your cell
- Social media, search results
- Electronic tax returns



Who locks digital accounts upon death or disability?

When all digital assets are known, new products are needed.

Provide more Peace of Mind during estate planning.

Create an Inventory – What did we Miss?

- Family and professional contacts
- Estate planning documents (wills, trusts)
- Instructions for smartphone access
- Identity theft protection subscriptions
- Social security, Medicaid benefits
- Complete, correct and current access codes
- Data and documents in both digital or tangible formats

How will an executor gain access upon death or disability?
Technology-driven estate admin is personal & cost-effective.
Offer more account closure services for value-add.

Convert Inventory to Digital

BEFORE…

…AFTER

Use Digital Inventory for Ultra Planning

(Trust and Estate Administration Support After Death or Disability)

- Financial - banks, brokerage, investment, retirement and trust accounts
- Insurance - life, property, auto, pre-need, long-term care / disability
- Loan documents, private investments, real estate, promissory notes
- Patents, trademarks, web domains
- Retirement, annuities, pensions
- Scheduled deposits and payments
- Social media and search results…and more

Account discovery and closure should not be this difficult.
Differentiate & provide admin support using technology.
Learn more about your Clients and their digital assets.

Include Digital Property Protection Planning in Every Conversation

Identify your digital property today!

Thank you.

Betsy L. Ehrenberg
betsy@legacy-concierge.com
(650) 380-0688

What is Ghosting?

It may not be what you envisioned, but apparently there can be life after death. It's called "ghosting," and it's both scary and surprising.

Ghosting is a form of identity theft. It occurs when someone uses the personal information of a dead person, often for monetary gain. A savvy criminal can take over bank accounts, apply for new credit cards, and even file for fraudulent tax refunds. Ghosting often happens shortly after someone dies, before the death is widely known. That's because it can be months after a person dies before entities like credit reporting agencies, the Social Security Administration, and the IRS receive, share or register death records.

Some 2.5 million identities are stolen each year; over 320,000 thefts or about 13% are from deceased individuals. And you need only look in the obituary section of your local newspaper to see where identity thieves find the information they need. There, they can obtain a potential victim's full name, maiden name, date of birth, place of birth, place of residence at death, mother's maiden name, and even where the victim went to school and was employed.

With that information, it's often not difficult to track down additional information online, such as the deceased's home address. And given the number of data breaches involving Social Security numbers, it's possible an identity thief could track that number down, as well, perhaps purchasing it from another criminal.

Criminals can often get away with ghosting because no one may be aware anything fraudulent is going on. The deceased can't check their credit reports for unfamiliar activity and credit protection services are discontinued as of date of death.

How can you help protect your family from ghosting? These tips may help:

- Limit the amount of personal information you share about the deceased in newspaper and online obituaries.
- Notify the Social Security Administration of the death. In most cases, this is handled by the funeral home handling the arrangements.
- Send the IRS a copy of the death certificate so that the agency can note that the person is deceased. The death certificate may be sent to the IRS office where the deceased would normally file a tax return; however there are two IRS office locations for every state depending on whether the person owed money or not.
- Send copies of the death certificate to each credit reporting agency asking them to put a "deceased alert" on the deceased's credit report.
- Review the deceased's credit report for questionable credit card activity.

Losing a loved one is difficult enough. By taking a few simple steps after a family member's death, you can help by locking their accounts and removing their name from a number of sites. You will protect their identity and, in doing so, help protect the family from further emotional suffering. For a complete package of estate protection services, please contact Legacy Concierge at sales@legacy-concierge.com today.

LOCKYT

We put the details to rest

GRAVE ROBBING IN THE 21st CENTURY

In today's increasingly connected world, identity theft has become a serious problem. It is estimated that 17.6 million Americans are the victims of some form of identity theft every year. Of those attacks, 2.5 million happen to someone who is deceased. This means 2,200 deceased Americans every day will be deliberately targeted and have their identities stolen. Another 1.6 million Americans will have their identities stolen by chance when fabricated Social Security numbers happen to match those belonging to deceased individuals. Identity thieves fraudulently apply for loans, drain bank accounts, open credit cards, and even establish cell phone plans, according to research conducted by ID Analytics. Identity theft is the 21st century's version of grave robbing.

When a loved one passes away, worrying about protecting their identity or erasing their electronic footprint isn't usually a family's top priority. On average, an American has over 150 locations where their electronic footprint is residing. The electronic footprint is composed of electronic records, and digital assets. Identity thieves who target the deceased are cunning and relentless, and often use obituaries to obtain Social Security numbers, previous addresses, birthdays, employment histories, and other information that they then use to drain the deceased's current accounts, file false tax returns, open new credit accounts, and accrue tremendous debt.

Identity theft has never been more rampant than it is now, which is why it's so important to know what can be done to avoid it. The best way to protect posthumously vulnerable information is to be prepared, since it can take up to 6 months for financial institutions, credit bureaus, and the Social Security Administration to update their records to reflect that the account holder is deceased.

Steps to Prevent Identity Theft Before Death

Request a credit freeze. This will block any identity thieves from opening up new lines of credit. Your credit may be frozen and unfrozen as many times as is needed, without penalty.

Choose a trusted executor. This is the person or institution you put in charge of administering your estate and carrying out your final wishes. Picking the right executor can help ensure the prompt, accurate distribution of your possessions with minimal family friction. Whoever you choose to serve as your executor, be sure to get their approval before naming him or her in your will. And once you've made your choice, go over your financial details in your will with that person, and let them know where you keep all your important documents and financial information.

Keep your will up to date. Be sure to make updates to your will if there are any major life changes like moving, marital status changes, having a child, etc. It is also very important to let your executor know where the latest copy of your will is located. Things can get very complicated if any major life events have happened since the last will was created.

Assemble a complete inventory of all assets physical and digital, so that an executor will know where you have assets. Make sure to keep this list updated and in a secure location, but do not include passwords or logins. This will help estate executors to know which accounts to shut down and continue monitoring, and will also alert them as to which entities need to be notified of one's death.

Steps to Prevent Identity Theft After Death

Limit the information in an obituary to what is needed to honor the deceased, but not to expose a credit profile for an identity thief. Avoid including personal information such as the birthdate, home address, or mother's maiden name.

Freeze the deceased's bank accounts, notifying their financial institutions that the account holder has died, and the accounts are to be frozen pending further instructions from the executor**.** When communicating with these companies, maintain a documented trail of communication for your records.

Close down avenues, which can make it easier to fake an identity. All funeral homes notify the Social Security Administration (SSA) of the death, so if that person was getting their benefits deposited in a financial institution, the SSA notifies the bank or credit union. The SSA will also inform TransUnion, one of the three main credit bureaus. However, you will need to contact the appropriate state's Department of Motor Vehicles and the other two main credit bureaus, Equifax and Experian. Also, be sure to remove the names of the deceased from any accounts where they are listed as joint account holders. Physical credit cards, driver's licenses, and passports should all be destroyed.

Identify accounts unknown to the estate executor and shut those down too. Unfortunately, many people don't have accurate lists of all of their accounts and/or don't give them to their estate executor. Therefore, it becomes necessary to proactively search, identify, and freeze accounts that are not known to the estate executor.

Unfortunately, there is no way to 100% protect deceased loved ones' identities, since identity thieves won't be scared away by garlic or wooden stakes. However, with a little preparation, it is much easier to keep a deceased loved one's identity safe from theft.

Bio for Betsy

Betsy Ehrenberg is a business leader and innovator in the tech industry. She has successfully started, built and sold two software companies. Her first Silicon Valley venture was Operations Control Systems, a software company providing performance and security services to Fortune 50 companies that was later sold to Cisco Systems, Inc. In 2003, she founded Veriden, providing biometric identification to secure financial transactions in the payment processing space. In addition to her business acumen for software companies, she has also and founded two non-profits providing art business education.

Currently Betsy is the CEO and Founder of Legacy Concierge, a revolutionary cloud-based software service platform that manages an individual's asset and electronic footprint by creating an electronic vault of all their digital assets. Upon death, the platform facilitates the removal of the deceased's digital footprint, thereby helping to prevent identity theft and preserve financial accounts. Legacy Concierge operates nationwide and currently maintains notification protocols for government agencies and private enterprises.

Betsy is a winner of the Woman of the Year – Business in Santa Clara County (Silicon Valley) award, she has also presented as a Keynote Speaker at the Association for Computer Operations Management, and at Washington DC's Security Symposium on Biometric Identification.

For more information about Legacy Concierge or Betsy, visit www.legacy-concierge.com

Case Focus

On October 16, 2017, the Massachusetts Supreme Judicial Court issued ***Ajemian v. Yahoo****!, Inc.,* 478 Mass 169 (2017), which holds that federal law, specifically the Stored Communications Act, does not prohibit an email service provider from disclosing email content to a decedent's personal representative. This ruling is significant to the fiduciary community in Massachusetts because it helps define post mortem ownership of digital assets.

Background

The issue in ***Ajemian v. Yahoo*** arose after John Ajemian died from a cycling accident. His brother and sister were appointed personal representatives of his estate. The personal representatives knew that their brother had a personal Yahoo email account, which they wanted to access as part of the estate settlement process. Yahoo refused their request for access and refused to disclose the account's contents, citing what Yahoo considered to be a prohibition on disclosure imposed by the federal law known as the **Stored Communications Act** (18 U.S.C. §2701 et seq.)(the "Act").

The Act was enacted in 1986 to create Fourth Amendment-like privacy protection for email and other digital communications stored on the internet. It limits the ability of the government to compel information from internet service providers. In addition, it restricts internet service providers' ability to reveal information to nongovernment entities. Both civil and criminal penalties are provided for violations of the Act. The Act protects the privacy of users of electronic communications by making unauthorized access to electronic communications a criminal offense.

Yahoo claimed that the Act prohibited it from disclosing private emails to the personal representatives unless a specific statutory exception applied. According to Yahoo, no such exception applied in this instance. In addition, Yahoo maintained that the terms of service agreement that the decedent had agreed to when he created the email account gave Yahoo the discretion to refuse the personal representatives' request. As a result, Yahoo was concerned with potential liability if it turned over the contents of the decedent's email account to personal representatives absent specific authority in the the Act.

Yahoo prevailed in the probate court, which held that the requested disclosure was prohibited by the Act. The court also concluded that although the estate had a common-law property right in the account's contents, disputed issues of material fact concerning the application of the terms of service agreement precluded summary judgment.

The SJC Decision

The SJC held that the Act did not prohibit Yahoo from voluntarily disclosing the contents of the account's email communications to the personal representatives because the Act contains an exception that allows disclosure based on **lawful consent** (citing Section 2702 of the Act). The personal representatives argued that they could consent to release of the account's contents because the account was property of the estate and therefore receiving the account's contents would effectively allow them to take possession of estate property in their normal capacity as personal representatives. In contrast, Yahoo argued that under the Act lawful consent could come only from the account's actual, original user.
The SJC disagreed with Yahoo and held that Yahoo's interpretation of lawful consent would preempt state probate and common law, specifically state law allowing a personal representative to provide consent on behalf of the decedent, without any clear congressional intent to do so. The SJC, however, held that while Yahoo *may* divulge the content of the decedent's communications, Yahoo is *not required* to do so if its terms of service agreement provided otherwise.

On the issue of whether Yahoo could the use the terms of service agreement with the decedent to limit access to the account by the decedent's personal representative, the SJC divided. Yahoo argued that the terms of service agreement granted Yahoo the right to deny access to, and even delete the contents of, the account at its sole discretion, thereby permitting it to refuse the personal representatives' request. Over Chief Justice Gants' objection, the Court remanded that issue to the probate court for further proceedings on whether the terms of service agreement is an enforceable contract.

Justice Gants assumed for purposes of the opinion that the terms of service agreement is enforceable against the estate. Justice Gants further noted that the terms of service agreement grants Yahoo the right to terminate the agreement and the user's access and to remove and discard any content within the service's possession. Yahoo, however, could not contend that the termination provision gave Yahoo an ownership interest in the user's content. Therefore, even if the terms of service agreement limits the estate's property rights, Yahoo cannot claim ownership over the content still retained by Yahoo. Nor could the termination provision be reasonably interpreted to allow Yahoo to destroy emails after the personal representatives initiated a court action to obtain the messages. Justice Gants noted it was unfair to put the estate through the expense of another court proceeding and dissented from the majority's decision to remand the case for further proceedings regarding the terms of service agreement.

Key Takeaways and Possible Future Developments

Given that this case has been remanded, it is far from concluded. However, even though the decision does not order Yahoo to disclose the emails to the personal representatives, the decision negates the email industry's position that the Act prohibits disclosure. In and of itself, that is significant for personal representatives who seek access to internet communications of the deceased individual's estate that they are administering.

Presumably, the Massachusetts probate court, on remand, will simply issue an order mandating disclosure, now that the SJC has confirmed that the personal representative may provide lawful consent under the Act. But what if the probate court, on remand, does *not* order the disclosure, and instead agrees with Yahoo that its terms of service agreement allows the company to destroy or withhold the emails? Chief Justice Gants indicates that if the trial court were to hold that Yahoo's terms of service agreement were binding on the parties and permitted Yahoo to destroy the decedent's email messages, the SJC "would surely reverse that ruling."

Practitioners have begun to include specific authorizing language in their estate planning documents that addresses a fiduciary's rights relative to an individual's digital assets. These explicit directions should squarely address the lawful consent exception raised by the Act.

The SJC also suggested, in a footnote, that nothing precludes the Legislature from regulating the inheritability of digital assets. A majority of states have addressed the issues presented by *Ajemian* by enacting the **Revised Uniform Fiduciary Access to Digital Assets** Act ("RUFADAA").

RUFADAA was drafted through a collaborative effort between fiduciary professionals and internet service providers. RUFADAA extends the traditional power of a fiduciary to manage tangible property to include management of a person's digital assets. As a compromise between the drafting parties' interests, RUFADAA allows fiduciaries to manage digital property, but restricts a fiduciary's access to electronic communications such as email, text messages, and social media accounts unless the original user consented to this access in a will, trust, power of attorney, or other record.

There are currently several bills pending before the Massachusetts Legislature relating to varying forms of access by fiduciaries to digital assets. A Massachusetts Study Committee has recommended the adoption of RUFADAA in Massachusetts, but as of yet, RUFADAA has not been formally filed as a bill in the Commonwealth.

Mary H. Schmidt, Esq. is a partner at Schmidt & Federico and is a member of the Massachusetts Ad Hoc RUFADAA Study Committee. Colin Korzec is a National Estate Settlement Executive at U.S. Trust, Bank of America Private Wealth Management and Chair of the Massachusetts Ad Hoc RUFADAA Study Committee.

End of case study report.