# WHITE PAPER

## Protecting Digital Assets

BY **BROOK H. LESTER, CPA,**
PRINCIPAL & CHIEF WEALTH STRATEGIST

Each year, new technology moves seamlessly into our lives. With it comes added convenience, new modes of entertainment, and more ways to communicate and share. Little by little, our footprint in the digital space grows. We tend not to realize just how large our footprint is until something happens to compromise or complicate some aspect of our online lives, revealing just how vast and complex the digital sphere is.

Regulations, laws and policies governing the sharing and protection of data are constantly changing to keep pace with the rapid transformation in the digital domain. It has made the concept of "ownership" of one's information increasingly more complex, and has also led to challenges with cybersecurity and an era of cybercrimes.

continued on next page ›

DIVERSIFIED TRUST
COMPREHENSIVE WEALTH MANAGEMENT
diversifiedtrust.com

From paying bills to connecting with friends, many daily activities are taking place on online platforms. This can also include asset management. As you take steps to protect your assets and create a will, it is important to extend those considerations to your digital assets to help avoid challenges that are inherent with data ownership.

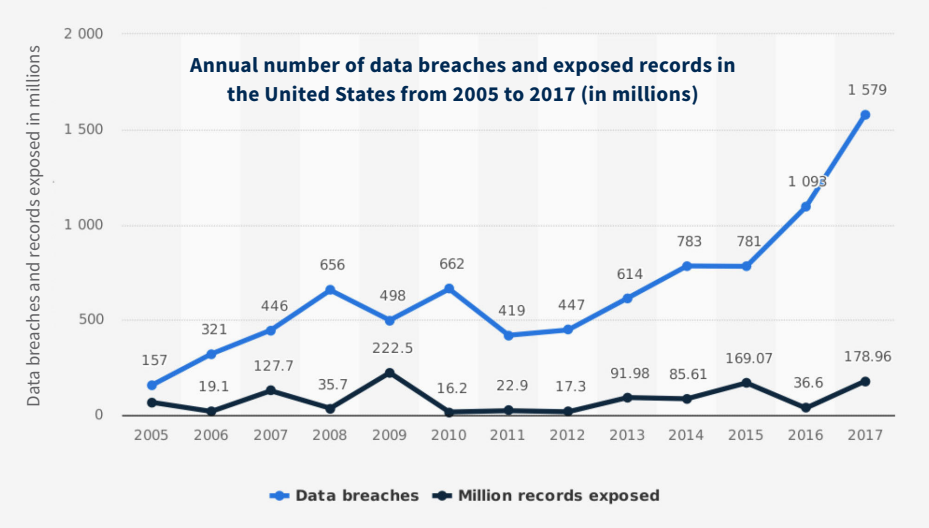
## What Are Digital Assets?

While financial assets typically include shares, property or policies, digital assets are stored content or accounts that live in the digital space. Social media accounts, photos and music are digital assets, as are emails and text messages as well as credit card, online banking, healthcare and bill pay accounts, to name a few. You may not have considered these as "assets" because they don't have a monetary value or you don't view them as "yours." However, they all qualify as your digital assets and are worth the same degree of protection as your financial assets.

## The Value of Your Digital Assets

Digital assets often contain a great deal of personal information. Your complete identity – social security number, health information, financial information, and likeness – is now online. A security breach or leak can result in this information getting into the wrong hands. Criminals can use your information to file taxes, open credit cards, and make purchases.

Cybercrimes are expected to continue to increase, according to Verizon's 2018 Data Break Investigations Report, and 2018 has already experienced 53,000 cybersecurity incidents and 2,216 data breaches. Therefore, it is imperative that you know the proper steps to protect your information, as well as what to do if someone has accessed your personal information.




**Sources**
Identity Theft Resource Center: CyberScout
© Statista 2018

**Additional Information:**
United States; Identity Theft Resource Center; CyberScout; 2005 to 2017

Source: Statista: Pew Research Center Study

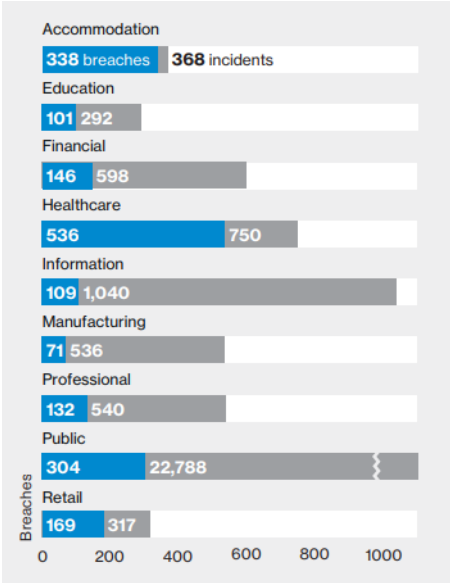
continued on next page ›

You may believe that your text messages and photos are of little interest to others or your iTunes library is only worth several hundred dollars at best, but they have more significance than you might think. Texts, photos and emails might contain valuable information, either about your personal life, or log-in information. Or, they may have sentimental value that your family might like to access upon your passing. However, when you die, your family does not have guaranteed access to any of these assets. Your digital assets should be a part of estate planning, so that loved ones have permission to access your information but still provide protections from others gaining undesired access to your information.

## A Digital Safe: How to Guard Online Assets

Protecting your digital assets is a matter of online vigilance. Operating as if anyone could potentially access your personal information and utilize it for their own benefit is the best way to ensure you don't fall victim to crimes, at least those within your control.

**Number of incidents and breaches by sector**




Source: Verizon: 2018 Data Breach Investigations Report

Keeping software up-to-date on all devices ensures that you stay current with the most advanced security settings possible. Developers constantly work to improve the functionality and security of their software, which is why you receive regular update notices to download the latest software. Taking the time to initiate that download could protect your assets from hackers.

Be sure to protect your passwords by using multi-factor authentication, making it difficult for an unauthorized log-in, and choose complex passwords or passphrases for all your accounts. Multi-factor authentication provides an additional level of data security in addition to a username and password. If you've ever used a numerical code or connected the dots on your smart phone, that step is an example of multi-factor authentication. Never store your passwords in an easily accessible/physical location, such as on a note stuck to your laptop or in a desk drawer next to your laptop. If you need help remembering them, use a secure password manager such as LastPass or Dashlane.

dashlane LastPass

continued on next page ›

Another way you can prevent outsiders from seeing your personal information is by ensuring that you are using an encrypted website. These sites scramble the information so that it is not easily intercepted. You can verify that it's an encrypted site if the URL begins with https. It is also generally safer to type a URL into a browser instead of clicking a link in an email, in case the email happens to be part of a phishing scam, an attempt to obtain private, sensitive information from your electronic accounts. For example, when you get an email notice to pay a bill, type the website URL into a new window rather than clicking "Pay My Bill," since you will be entering personal information into that site. If you open a scam attachment, you may be granting a hacker access to your computer.

Other good online practices include:

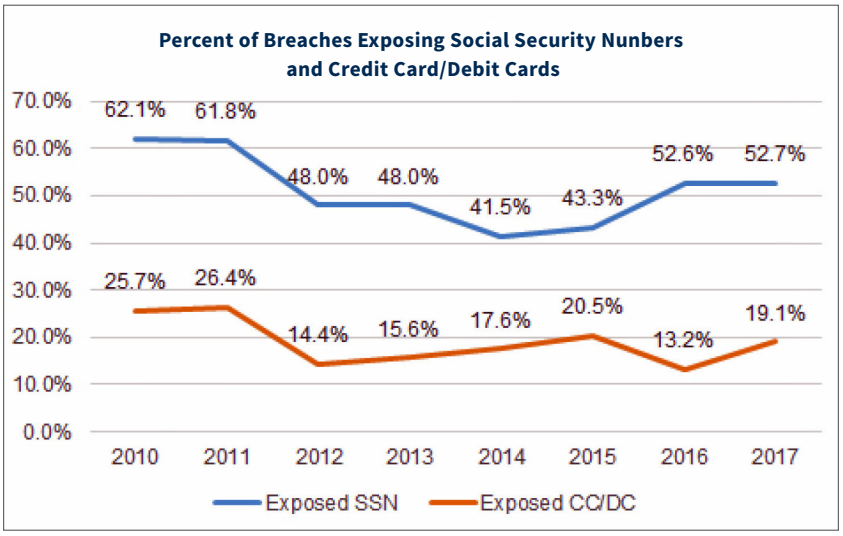
- **backing up files;**
- **installing security software;**
- **using firewalls;**
- **securing your wireless network;**
- **protecting your laptop to avoid theft and;**
- **paying attention to security warnings.**

Finally, when disposing of or recycling electronics, such as older cell phones or laptops, use a verified vendor to ensure that your hard drive will be wiped clean.

continued on next page ›

## Avoiding Virtual Crimes

Despite your vigilance, your digital assets may fall into the wrong hands as a result of a data breach or an adept virtual criminal. The Federal Trade Commission (FTC) has a number of resources available for consumers at **consumer.ftc.gov** to guide you in the event that your identity has been stolen.




Source: Identity Theft Resource Center: 2017 Annual Data Breach Year-End Review

If you notice or are made aware of suspicious online activity, call the companies where fraud has occurred and either freeze the account or close it entirely. Change all of your passwords, not just those on compromised sites, and implement any additional security protections, such as the aforementioned multi-factor authentication, if you haven't already.

Contact one of the three credit bureaus – Experian, Equifax or TransUnion – and place a free 90-day fraud alert on your credit report. That bureau will then notify the other two. Then report the fraud to the FTC at **IdentityTheft.gov**.

Once you have tackled the reporting process, you will then begin the arduous process of clean-up. Critical steps to consider include:

- **closing any and all new accounts;**
- **removing bogus charges;**
- **working with credit bureaus to correct credit reports and;**
- **Implementing an extended fraud alert or credit freeze.**

continued on next page ›

Identity theft is an unnerving ordeal, but there are many resources to help guide you through it. And above all, try to stay calm.

## Securing Your Digital Rights

It is likely that you have either undertaken or considered estate planning so that your financial assets can be allocated appropriately upon your death. Unfortunately, your digital assets cannot be handled quite as simply. Digital assets are not automatically distributed to your next of kin. This is because many digital companies view their websites or social networks as licensing properties, which expires when the licensee dies.

Yahoo!, for example, terminates all your digital information upon death. To access a relative's Facebook page, you must get a court order. With the introduction of Digital Asset Protection Trusts (DAP Trusts), though, a trust creator can now place existing digital rights and property, including that license, into a trust for beneficiaries to use. You just have to be sure you plan ahead.

Begin by creating a list of all of your digital assets and assign a value to them. While you may think that a photograph does not have much financial worth, domain names, music libraries, online businesses and bitcoins are valuable digital assets. You must also consider things like PayPal balances, credit card rewards and online credits. These all have monetary value and are elements of your portfolio that require special instruction.

Make a list of all of the usernames and passwords required to access these digital assets. **Do not include this information in your will, as that document becomes public upon your death.** Draft a hard copy and put it in your safe deposit box or put it in a password-protected document that can be accessed by trusted family members. Just be sure to make the master password accessible to a designated family member or executor.

continued on next page ›

### Important Notes And Disclosures

This White Paper is being made available for educational purposes only and should not be used for any other purpose. Certain information contained herein concerning economic trends and performance is based on or derived from information provided by independent third-party sources. Diversified Trust Company, Inc. believes that the sources from which such information has been obtained are reliable; however, it cannot guarantee the accuracy of such information and has not independently verified the accuracy or completeness of such information or the assumptions on which such information is based. Opinions expressed in these materials are current only as of the date appearing herein and are subject to change without notice. The information herein is presented for illustration and discussion purposes only and is not intended to be, nor should it be construed as, investment advice or an offer to sell, or a solicitation of an offer to buy securities or any type of description. Nothing in these materials is intended to be tax or legal advice, and clients are urged to consult with their own legal advisors in this regard.

The next step in preparing for the future of your digital assets is to draft a statement articulating who will control each of them after your passing. Be aware, though, that even though your wishes are written, the executor is not guaranteed access. Many digital platforms consider a log-in with someone else's password a violation of their terms. Online data management companies have begun selling services that claim to transfer digital assets to your beneficiaries, but they don't resolve the potential conflicts with online providers' terms of service or federal laws.

Recently, a group of lawyers drafted the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), which allows people to specify in their wills that the executor of their estate can access their email and social media profiles. Thus far, 39 state legislatures have adopted it. However, even that law doesn't specify exactly how that access should happen, so the executor must still contact the company behind each platform.

The rules for digital estate planning are just now beginning to be developed, so it's important to be vigilant in planning ahead. Not preparing for the fate of your digital assets could prevent loved ones from accessing precious memories, or more seriously, result in a lapse in payments and leave you vulnerable to post-mortem identity theft.

## Plan for Sharing Your Digital Assets with Trusted Sources

The expansion of our digital sphere is an exciting, yet risky, process as advancements in entertainment, communication and sharing will require constant upgrades in data security and protection. While the threat of increased cybercrimes is daunting, taking the proper steps to understand your digital assets, establish your digital rights and upgrade your online security will decrease the chances of identity theft and provide peace of mind.

ATLANTA

400 Galleria Parkway, Suite 1400
Atlanta, GA 30339
*Phone:* 770.226.5333

GREENSBORO

300 N Greene Street, Suite 2150
Greensboro, NC 27401
*Phone:* 336.217.0151

MEMPHIS

6075 Poplar Avenue, Suite 900
Memphis, TN 38119
*Phone:* 901.761.7979

NASHVILLE

3102 West End Avenue, Suite 600
Nashville, TN 37203
*Phone:* 615.386.7302