Winter 2021/2022

Estate Planning Update Winter 2021/2022 - Identity Theft and Data Breaches: An Ounce of Prevention Is Worth a Pound of Cure

Undertaking sound estate planning involves the disclosure of sensitive personal and financial information to trusted advisors. Protection of that information has become a significant concern in a world where information is transmitted and stored electronically and illegal breaches make the headlines seemingly daily. These concerns grow where an estate includes digital assets that never existed only a few decades ago. As a result, being mindful of the risks of data breaches and understanding the need for protection of your electronic information have become important issues for all our clients. Earlier this year, in its annual Consumer Sentinel Network report for 2020, the Federal Trade Commission (FTC) announced that cases of identity theft skyrocketed during the COVID-19 pandemic, with reported incidents increasing 100 percent since 2019. Unfortunately, in 2021, a new surge in phishing, ransomware and supply chain attacks points to another record-breaking year for data compromises. According to the Identity Theft Resource Center, the number of publicly reported data compromises through September 30, 2021, already has exceeded the total number of events in full-year 2020 by 17 percent. Identity theft or identity fraud happens when a thief gains access to personal information—such as name, address, credit card or bank account numbers, Social Security number, phone or utility account numbers, passwords, or medical insurance numbers—and uses that information for their economic gain. COVID-19 appears to have provided new fuel for cybercriminals, who have been preying upon the public's concern about this global crisis. Recent scams are designed to trick people into sending money, to disclose personal information or to click on emails and websites that deliver computer malware onto the recipients' computer or network. Over the past 24 months, our clients have been affected by criminals seeking personal information by:

- impersonating a representative of a bank or other financial institution providing or requesting information about our client's account;
- seeking donations for purported charitable causes related to COVID-19;
- taking advantage of the recent increase in work-at-home arrangements by impersonating legitimate business correspondence; and
- posing as a government organization claiming to provide information about COVID-19, such as through heat maps or infographics.

Others have experienced significant actual or potential loss through:

- extortion by threats to disclose embarrassing or extremely personal information or pictures stolen from a personal computer;
- ransom demands in exchange for passwords to decrypt information stored on a personal computer or home network;
- redirected wire transfers arising from man-in-the-middle attacks;

- fraudulent claims for unemployment insurance filed in multiple states using stolen personal information; and
- the opening of fraudulent bank accounts and lines of credit using stolen personal information.

These and other types of incidents have the potential to cause tremendous financial, emotional, physical and social harm to the victims. In the event our clients are affected by identity theft or fraud, we encourage them to react quickly by promptly reaching out for expert assistance. Some homeowners insurance and other service providers offer a range of identity restoration services and indemnity coverage to address the immediate potential for financial harm. In most instances, relying on guidance from your insurer's panel of experts or an identity restoration service provider can be cost-effective and efficient. For more complex situations, however, you may need a more customized approach. Your attorney or financial advisor will likely be able to point you in the right direction. For our clients, depending on the situation, we offer a self-help guide or a bespoke hands-on service to address each client's specific situation. For those identity theft victims who are prepared to act on their own, we recommend visiting the FTC identity theft website for a step-by-step reporting and recovery guide to help them cope with the many challenges they may face. Our bespoke service includes providing an interface with private investigators, law enforcement authorities and others to address victims' immediate and long-term concerns. Of course, the best way to reduce the risk of being affected by identity theft or fraud is to apply an ounce of prevention. We offer a few preventive tips:

- **Freeze your credit.** Freeze your credit files for free with Equifax, Experian, Innovis, TransUnion and the National Consumer Telecommunications and Utilities Exchange. Credit freezes prevent someone from applying for and getting approval for a credit account or utility services in your name.
- **Secure your Social Security number (SSN).** Don't carry your Social Security card in your wallet. Only give out your SSN when truly necessary.
- **Protect your personal information.** Don't share personal information (birthdate, Social Security number or bank account number) just because someone asks for it.
- **Collect mail every day.** Place a hold on your mail when you are away from home for several days.
- **Pay attention to your billing cycles.** If bills or financial statements are late, contact the sender.
- **Review your credit card and bank account statements.** Compare receipts with account statements. Watch for unauthorized transactions.
- **Review your credit reports once a year.** Be certain that they don't include accounts that you have not opened. You can order reports for free from AnnualCreditReport.com.
- **Watch for impersonators.** Avoid clicking links in emails without hovering over them to see the destination first. Hang up and call a customer service line to verify a caller's identity. Don't trust caller ID on your smartphone.
- **Use the security features on your mobile phone.**
- **Maintain password security.** Create complex passwords that identity thieves cannot guess. Change your passwords if a company that you do business with experiences a breach of its databases. And use different passwords for each of your online accounts.
- **Use MFA.** For important online accounts (e.g., bank accounts, email accounts), implement multifactor authentication (MFA).

- **Protect yourself on public Wi-Fi networks.** Update sharing and firewall settings when you're on a public Wi-Fi network. Use a virtual private network if you use public Wi-Fi.
- **Secure your home Wi-Fi network.** Configure your home Wi-Fi network with encryption and a secure password.
- **Protect against dumpster divers.** Shred receipts, credit offers, account statements and expired credit cards.
- **Store personal information in a safe place.**
- **Secure your personal devices.** Install firewalls and virus-detection software on your home computer, tablets and other devices.

Finally, we note that tax identity theft has proven to be a perennial issue for the IRS, especially during tax season, including due to cybercriminals committing tax refund fraud by filing taxes in the victim's name. In an effort to battle various flavors of tax fraud and tax-related identity theft, the IRS announced that, as of January 2021, it has expanded its Identity Protection PIN Opt-In Program to all taxpayers, assuming they can properly verify their identities. An Identity Protection PIN (IP PIN) is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. We encourage all our clients to take advantage of this IP PIN program. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool. Your best protection against identity theft or fraud is to remain vigilant. And if you are a victim of identity theft, you should reach out for assistance quickly.

For more Day Pitney alerts and articles related to the impact of COVID-19, as well as information from other reliable sources, please visit our COVID-19 Resource Center. COVID-19 DISCLAIMER: As you are aware, as a result of the COVID-19 pandemic, things are changing quickly and the effect, enforceability and interpretation of laws may be affected by future events. The material set forth in this document is not an unequivocal statement of law, but instead represents our best interpretation of where things stand as of the date of first publication. We have not attempted to address the potential impacts of all local, state and federal orders that may have been issued in response to the COVID-19 pandemic.