December 11, 2023

Estate Planning Update Winter 2023/2024 - The Good, The Bad, and the…Artificial? AI-Enabled Scams: Beware and Be Prepared

AI-Enabled Scams: A Growing Concern

Artificial intelligence (AI) is an exciting new technology that offers considerable promise in making much of our work more efficient. As with any new technology, it is important to focus on the dangers as well. The rise of AI-enabled scams presents a significant concern. Bad actors have already begun to exploit the capabilities of AI to create highly convincing and personalized fraudulent schemes. Understanding the nature of these schemes is crucial as we enter an era of readily available AI.

AI technologies have enabled scammers to craft highly targeted and believable fraud attempts. These include the following:

Personalized Phishing Attacks: Using data gathered from various sources, AI can tailor phishing emails or other messages to make them appear to come from trusted sources, such as family members, legal advisors or financial institutions. Senders may also impersonate IRS agents or other government employees. These messages might lead the recipient to disclose personal financial information or even transfer funds.

Deepfake Technology: AI can generate realistic videos or audio recordings, known as deepfakes. It is important to note that AI can be used to create voice messages or even live conversations using convincing simulations of the voice of a friend, advisor or family member. Similar to phishing attacks, these deepfakes can be used to induce the recipient to transfer funds or disclose confidential information. The novelty of this technology can increase the potential for people to fall for the deception.

AI-Powered Social Engineering: AI algorithms can analyze personal data and social media footprints in order to understand an individual's behavior and preferences as well as their professional circles and friend groups, making social engineering attacks more convincing. Scammers might use this information to manipulate individuals into disclosing confidential information.

To safeguard against these advanced scams, we all should continue to exercise vigilance and caution in any interaction involving the disclosure of personal information.

Verify Communications: Always verify the authenticity of any unexpected communication, especially if it involves sensitive information or financial transactions.

Secure Personal Information: Be cautious about sharing personal information online. Regularly update privacy settings on social media and other platforms to minimize the amount of data available to bad actors.

Consult with Professionals: If in doubt, clients should consult with their trusted advisors, preferably by phone, before acting on any communication that seems unusual or unexpected.

Stay Informed: Keep abreast of the latest types of AI-enabled scams. Awareness is a critical defense against falling victim to new and more sophisticated frauds.

The need to stay vigilant applies to us all. Day Pitney engages in a continuous process to educate all personnel on the risks of AI and update internal policies to protect client and firm information as threats evolve. At the same time, the firm continues to evaluate new technologies and investigate ways to harness AI technology, including to make the practice of law more efficient while prioritizing information security and maintaining our high quality of work. While clients may be tempted to ask AI legal questions and even use it to draft legal documents, AI apps themselves caution against doing so, recognizing that there is no substitute for the experience and skill of your living, breathing estate planning attorney. In sum, as with any new technology, AI presents both risks and opportunities, and caution is warranted as we all learn more about it.