AI & U

March 2026

TRUXTON
WEALTH • FAMILY OFFICE • BANKING

William "Hank" Stuart
Sr Managing Director
Truxton Banking
Email Hank
Link to Bio

"A, E I, O, U, and sometimes Y". Most of us well remember how our parents and teachers taught us the vowels of the English language. However, it seems like today the vowels of E, O, U, and sometimes Y have been relegated to the back row. Standing front and center and grabbing all the daily headlines are only A and I!

AI – Artificial Intelligence. Not a day passes that I do not hear at least 20 references to AI. Thirty-five years ago, a friend told me he was working at Vanderbilt in their Artificial Intelligence Department. I did not fully grasp what AI meant then, and I am sure I do not fully grasp all the AI implications and impacts that it has for us today. From an esoteric concept thirty-five years ago to a sudden entrance into our vocabulary and our day to day lives, AI is here to stay – front and center - for either good or bad.

Speaking of bad, AI and all its capabilities is now being used by the "bad guys" (fraudsters, cyber criminals, con artists, swindlers, crooks) for very bad purposes, stealing billons of dollars every year from the "good guys" – men and women who work hard all their lives to have a nest egg of assets. Although there have always been bad guys going after those nest eggs, AI has given them another tool in their very bad toolbox.

The latest AI tool the bad guys are using is to clone voices with alarming accuracy. You may be thinking – what possible harm could result from a cloned AI voice? By capturing 3-10 seconds of your voice, the bad guys can use AI to impersonate you and call your local bank or brokerage house to place an outgoing wire, close an account, or access online portals. Or the bad guys can use AI to impersonate bank personnel and attempt to gain enough information to set up fraudulent transactions. Federal Reserve Governor Michael Barr said in April 2025: "Deepfake attacks have seen a twenty-fold increase over the last three years."

The result of these deepfake attacks: FBI recorded (and who knows how much in unrecorded losses) $16.6 billion in cybercrime losses in 2024. That is $45 million a day in bad guy thefts from the good guys.

At Truxton, the security of your assets is our highest priority. That is why we have procedures in place to confirm that those proffering to be our clients are in fact our clients. An example – mandatory call back to our clients at their number on file verifying wires and ACH transfers, address changes, password resets, or adding new signers or beneficiaries. Our colleagues are trained to recognize those deepfake red flags. To use a wood working best practice – "measure twice and cut once" – our colleagues intentionally slow down and in essence "measure twice" to minimize the risk of our client's falling victim to the bad guys.

But banks, including Truxton, cannot do it alone. The good guys need to be consistently informed and educated by their banks of the dangers in this new AI age. (Thus, the purpose behind this article!) **Truxton will never ask for your online banking password, PIN, or one-time codes over the phone, or by email, or by text.** The bad guys can spoof caller ID's so always slow down, "measure twice", and call your bank or banker back at their known number. Truxton bankers knowing our clients and our clients knowing our bankers will always be the best line of defense against the bad guys.

AI is gathering all the headlines these days. But let us continue to use PI – Personal Intelligence – better known as common sense – to thwart the bad guys' bad use of AI. ▪