BROADSTONE ADVISORS

Strategic Planning

Financial Fraud Awareness Extends Beyond Complex Passwords

(Your Financial Independence May Be in Jeopardy).

By Todd McDonald, AIF® Certified Family Business Specialist®

Financial advisors and wealth managers (including the writer of this article) love to talk about asset allocation, introducing private markets into a portfolio, methods to produce income and grow your assets, each of these components, along with understanding the fee structure of your investment accounts contributes to financial freedom. ***Be forewarned!*** An investor and successful entrepreneur can accumulate significant wealth throughout their lifetime only to have a portion (or all) of their net worth accessed and lost by nefarious and fraudulent sources. Read on for a few examples of fraud, estranged family relationships and ways to protect your assets.

An important tenet of protecting your assets from bad actors is to **STOP AND THINK** about a conversation, financial request or suspicious activity. Trust your intuition; if you feel the management of your financial resources may place you in jeopardy or feels uncomfortable, hang up the phone, report a suspicious email and notify a trusted individual of the activity.

Over the past several years, in our financial practice, we have seen the devastation caused by a bad actor gaining inappropriate access to family and business assets. The damage often extends beyond simply financial loss to encompass irreparable rifts in family relationships. Sometimes individuals you trust are the sources of financial infidelity:

- A trusted family member accessed several million dollars worth of funds held in trust for the benefit of aging in-laws and their grandchildren, resulting in significant financial losses and adverse changes to the family dynamic. To make matters worse, the funds were accessed by a family member who is also an attorney. The attorney and his wife are divorcing.
- Assets from a single aging parent were accessed by one of her daughters who is her primary caregiver. Her sister lives several hundreds of miles from her family and discovered the fraud through banking records. The aged mother is the center of the controversy; the sisters' relationship has deteriorated and their children rarely interact.
- A busy, successful contractor and entrepreneur had more than $1,000,000 accessed from his 401(k) account by a sophisticated, fraudulent network. The funds were never recovered from the network, and insurance coverage fortunately indemnified the account of the contractor. The victim's confidence has been shaken and he feels vulnerable in his business dealings.
- Brothers operating a business relied on each other, however one brother accessed more than $1,000,000 of business assets for his personal use. The brothers no longer have a relationship and the fourth-generation business was sold to a third party.

Recently, I had the opportunity to connect with Kurt T. Strassberger, Senior Investigator in the New York State Police, Financial Crimes Unit located in Albany, New York. Kurt is also a

Certified Public Accountant. His credentials and experience as a forensic investigator enable him to provide useful information in creating financial awareness and tools to protect your assets. The New York State Police is engaged in outreach to their community, in an attempt to inform members of the public of the types of financial fraud that threaten them and stimulate a heightened awareness of ways to protect your assets.

According to Investigator Strassberger, "loneliness can be a powerful weapon." In addition to romance scams, an increasing amount of fraud is committed through business and personal email compromise, fraudulent "tech support" misappropriation of personal information and change in payments compromises for third-party payments to businesses.

Indicators of Financial Abuse:

The following can be important signs of impending or active financial fraud:

Controlling Behavior:

A family member, friend or neighbor forcing an individual to hand over paychecks or benefits, controlling personal spending and restricting access to bank and investment accounts or credit cards.

Economic Exploitation:

A third party gaining control of an ATM card, forging signatures, or creating debt in your name without permission.

Withholding Necessities:

Denying money for or access to essential items like food, clothing, or medication, creating a system of dependency.

Surveillance/Anxiety:

Monitoring spending, demanding receipts and changing account access to banking, investment and credit card accounts to the joint name of the manipulator.

Manipulation:

Pressure to sign legal documents or a power-of-attorney against one's best judgement.

Warning Notices:

Unexplained or unexpected transfer of assets, notice of unpaid utility, credit card or tax bills and overdraft notices from your bank.

If you are approached in a manner that suggests the potential of financial fraud, you should ALWAYS verify the requestors' identity. As an example, when notifying individuals or business representatives of a potential fraudulent issue, Strassberger advises them to hang up the phone and call Troop G of the New York State Police to verify his identity. In other words, it is prudent always to question authority and ensure that it is legitimate.

Investigator Strassberger discussed several reasonable and simple methods to protect your assets:

- STOP AND THINK! Does this request make sense? Do you feel uneasy about providing information to the requestor?
- Create checks and balances, include trusted family members to review your financial affairs. Coordinate regularly scheduled investment reviews with your trusted investment, accounting and legal representatives.

- Adopt a “never send cash to anyone” policy! Bona fide requestors, including the Internal Revenue Service, utility or local government, will never ask you to send cash to settle a debt or invoice.
- Take time to consider if the request is reasonable. If you didn’t ask for information, the request is likely fraudulent. Do not respond to requests that require you to act immediately or in secrecy.
- Establish your unique online banking, credit and investment account access on a proactive basis. The process will enable you to create specific user identification and passwords associated with the email address you provide. If you do not create a profile, the door is open to create access to your financial resources by others.

Awareness of the potential risks is the first step in protecting your financial resources. The United States Government has established the Internet Crime Complaint Center [1], an excellent resource to educate yourself about financial crimes, file a financial complaint and report access to your financial resources. Project Shamrock [2] a California not-for-profit founded by former prosecutor Erin West, provides useful education about the structure of various scams and resources to protect your assets.

Taking control of your financial resources takes dedication that goes beyond the basic balance of equities and fixed income, addressing required minimum distributions from your IRA and when to claim your Social Security benefits.

Awareness of fraudulent activities can protect more than your assets and your savings; *your financial independence and your closest relationships are worthy of protection by questioning and controlling who has access to your financial information.*

Todd McDonald

AIF® Certified Family Business Specialist®

Founding Partner, Wealth Management Advisor

Office: 518.220.3061 | Cell: 518.365.9923 (Call Only) | tmcdonald@broadstoneadvisors.com

Broadstone Advisors, LLC
24 Century Hill Drive, Suite 102
Latham, NY 12110
518.220.3060

Learn More

[1] **Source:** Internet Crime Complaint Center (IC3), accessed March 31, 2026. https://www.ic3.gov/

[2] **Source:** Operation Shamrock, “Stopping Scams Together,” accessed March 31, 2026. https://www.operationshamrock.org/

CRN202903-10760850