Client Letter, October 2026

Fifty 200
Investment Management



Protect Your Assets from Digital Scams That Could Cost You Dearly

Even casual NFL fans are likely familiar with Kansas City's star tight end Travis Kelce.

Much like a reliable blue-chip stock in a portfolio, Kelce has provided the Kansas City Chiefs with a rare combination of athletic ability and intensity that has elevated the offense, provided stability and star power, and helped fuel multiple championship runs.

If NFL football isn't your thing, you may be aware that he recently married music superstar Taylor Swift after a courtship that lasted almost three years.

So, where are we going with this? Investment scams cost Americans billions of dollars every year. Despite his wealth, Kelce was among the victims of a Ponzi scheme that bilked investors out of $35 million. It's unknown how much they will get back.

But it isn't simply well-known athletes and high-profile individuals that can get conned out of their riches.

The FBI's annual 2025 Internet Crime Report recorded more than 1 million complaints last year, a figure that has more than tripled over the past decade. Losses totaled nearly $21 billion, roughly double the amount reported just three years earlier and up 26% from one year ago.

The average loss, according to the FBI: $20,699.

Those over the age of 60 should pay careful attention. Those in, or approaching, retirement recorded 201,266 complaints, with losses totaling $7.7 billion (up 59% from 2024), or an average loss of $38,500.

Below are the reported crimes that resulted in the greatest financial losses for victims. The figures on the left side represent total reported losses, while the figures on the right show losses reported by victims age 60 and older. A short description of each crime is included.

1. Investment fraud: $8.6 billion/$3.5 billion
This deceptive practice induces investors to make purchases based on false information. These can include Ponzi and pyramid schemes, cryptocurrency schemes, pump-and-dump schemes, or what might be called "too good to be true" scams.

2. Business email compromise: (BEC) $3.0 billion/$568 million
A scam targeting businesses or individuals working with suppliers and/or businesses regularly performing wire transfer payments.

3. Tech/customer support: $2.1 billion/$1.0 billion
A criminal poses as a tech support representative, offering to fix non-existent issues so they can gain access to your personal financial information, passwords, etc.

4. Personal data breach: $1.3 billion/$324 million
A leak/spill of personal data that is released from a secure location to an untrusted environment.

5. Confidence/romance: $929 million/$584 million
An individual believes they are in a relationship (family, friendly, or romantic) and is tricked into sending money, personal and financial information, or items of value to the perpetrator, or to launder money or items to assist the perpetrator.

Source: FBI Internet Crime Report 2025

How do I protect myself?

It's a dangerous world, but you can minimize your odds of becoming a victim with simple steps and precautions.

1. Investment fraud

- Be skeptical of guaranteed returns or the promise of high returns with little risk.
- Verify the investment and seller.
- Beware of urgency and high-pressure tactics.
- Be EXTREMELY leery of investment opportunities that arrive unsolicited via email, text messages, online dating sites, and social media. Our advice: avoid them.
- NEVER share personal information such as passwords and security codes.
- Watch for red flags such as secrecy or requests of payment through cryptocurrency or gift cards.

2. Business email confidence fraud

This occurs when criminals impersonate executives, vendors, clients, or employees. Their goal is to trick victims into sending money, changing payment instructions, or revealing confidential information.

- Confirm any requests by picking up the phone and calling a known phone number.
- Don't trust an email alone to authorize a wire transfer or changes to payment instructions.
- Be especially cautious when a vendor suddenly changes banking information.
- Follow established protocols used by your company.

3. Tech/customer support fraud

- Ignore unsolicited tech support calls, emails, texts, and pop-up warnings. Firms such as Microsoft and Apple will never call you and warn you that your computer has been compromised. These calls come from criminals.
- Never give a stranger remote access to your computer or device.
- Verify the company using an official phone number or website before taking action.
- Never pay for support services with gift cards, wire transfers, or cryptocurrency.

Similarly, the IRS, Medicare, and Social Security will never make unsolicited calls demanding payment by gift card, cryptocurrency, or wire transfer, nor will they threaten arrest or request sensitive information.

Oblige them and it won't be long before they find something else that they claim is askew and demand additional payments.

4. Data breach

- Use a different password for each account and change passwords regularly.
- Enable multi-factor authentication whenever possible.
- Be cautious about sharing personal information on social media.
- Review bank, credit card, and investment accounts regularly.
- Consider freezing your credit if your sensitive information has been exposed.
- If credit monitoring is offered by a legitimate firm following a data breach, take advantage of the service.

5. Confidence/romance scams

The criminal often spends weeks or months building trust.

Perhaps you've met that perfect person online, but they never seem to be able to meet, as they live in a different state or even out of the country. Then, once you've become emotionally invested, requests for money surface.

NEVER send money or financial information to an online romantic interest. Watch out for stories involving emergencies, travel problems, medical bills, or investment opportunities.

Bluntly, better a broken heart today than a broken heart and a drained bank account tomorrow.

Another internet crime is **phishing and spoofing**. While the financial losses tend to be smaller than some other scams, they generated the greatest number of complaints.

- Think before you click on an email or link.
- Verify the sender.

- Be cautious regarding requests for information.
- Keep devices updated with the latest virus protection, web browser updates, and operating system updates.
- Don’t share passwords or personal information, especially when asked to verify by unsolicited phone calls and emails.
- Monitor bank accounts.

Keep in mind that **phishing** tricks you into taking a risky action, while **spoofing** makes a message appear to come from a trusted source.

The good news is that a healthy dose of skepticism can be one of the best defenses.

Be cautious. You don’t have to answer that phone call from an unknown number, especially if it originates from an unfamiliar area code. That’s what voicemail is for.

If you receive an unsolicited text from an unknown number asking friendly questions or claiming they found your number in their contacts but don’t know who you are, ignore it.

These messages are often designed to start a conversation and gain your trust before initiating a scam. You’re under no obligation to engage. Simply delete the text and block the sender.

Protecting your accounts, personal information, and digital identity is every bit as important as managing your portfolio. A few moments of caution today can help prevent a costly mistake tomorrow.

Tremors in treasuries continue

Last month, the economic and financial insights section was entitled, “Tremors in treasuries.” Judging by the bond market’s continued rise in yields, the ground is still shaking.

What’s going on?

During September 2026, the benchmark 10-year Treasury bond rose from a yield of 4.75% to 5.29%, the highest since 2002, according to the St. Louis Federal Reserve.

The 0.54 percentage point increase ranks as the 34th-largest monthly rise since 1962, placing it among the top 5% of all monthly changes over that period (St. Louis Federal Reserve data).

The 10-year is labeled the “benchmark bond” because it serves as the market’s primary reference point for interest rates across the economy, including mortgages, consumer loans, and business borrowing.

While it is difficult to quantify how much each factor is pushing yields higher, we can review the main reasons behind last month’s jump.

Key Index Returns[1]		
	September 2026 %	YTD %[2]
Dow Jones Industrial Average	-4.3	5.9
Nasdaq Composite	1.9	15.6
S&P 500 Index	-0.5	11.8
Russell 2000 Index	-5.4	12.7
MSCI World ex-USA[3]	-3.5	8.0
MSCI Emerging Markets[3]	-0.8	21.4
Bloomberg US Agg Total Return	-2.6	-2.9

Sources: Wall Street Journal, MSCI.com, Bloomberg, MarketWatch
MTD returns: August 31, 2026–September 30, 2026
YTD returns: December 31, 2025–September 30, 2026
1 It is not possible to invest directly in an index.
2 Annualized
3 In US dollars

Why are yields marching higher?

1. The Federal Reserve raised the fed funds rate in September, and investors believe additional rate hikes are ahead, according to a closely followed gauge from the CME Group.

   But the recent rise in Treasury yields cannot be explained by Fed policy alone. The forces driving the bond market are more complex.

2. The economy appears to be gaining momentum. The U.S. Bureau of Economic Analysis recently revised Q1 and Q2 GDP growth higher. Stronger economic activity lifts the demand for money (loans), putting upward pressure on the price of money (interest rates).

3. While it may be a secondary factor, the AI buildout is fueling hundreds of billions of dollars in new business investment. Some of that spending is being financed through the

bond market, and the increased demand for capital may be contributing to higher yields.

4. At the same time, the federal deficit remains large and growing, resulting in a steady flow of new Treasury issuance. That increasing supply of government debt may also be exerting upward pressure on yields as investors demand higher rates to absorb it.

5. Finally, concerns about inflation have not fully disappeared. If investors expect price pressures to persist, they typically demand higher yields to compensate for inflation's erosion of future purchasing power.

If yields are rising primarily because the economy is strengthening, that is not necessarily a cause for concern. In many ways, it reflects a self-correcting mechanism: higher rates can help cool an overheating economy, just as lower rates can provide stimulus when growth slows.

More worrisome are rising yields driven by persistent federal deficits or concerns that inflation may prove more stubborn than expected.

Even so, stocks have thus far largely withstood the surge in Treasury yields, as measured by the Nasdaq Composite and the S&P 500 Index. However, the Russell 2000 Index, which tracks smaller-cap companies, and the Dow Jones Industrial Average have run into a bit more resistance.

If you have questions…

Hopefully, you've found this review to be educational and helpful. If you have any questions or concerns about anything discussed above, please let me know. Please remember, the information shared in this letter is general in nature. You are urged to consult legal and tax professionals for advice specific to your situation.

Researched and drafted by Charles Sherry, MSc, for Horsesmouth. Editing and additional research by Sigma Financial Corporation / Parkland Securities, LLC. Past market performance is no guarantee of future investment performance or success.

Securities offered through Parkland Securities, member FINRA/SIPC. Fee-based investment advisory services offered through Sigma Planning Corporation, a registered investment advisor. Fifty200 Investment Management is independent of Parkland Securities & SPC.