



Financial *planner*



PARK PLACE WEALTH ADVISORS,
INC.

DANIEL J GANNETT

· 18 ORINDA WAY ORINDA, CA 94563 ·

DAN@PARKPLACEWEALTH.COM

· ORINDA – (925) 254-7766 ·

· SUNNYVALE – (408) 733-0245 ·

· FAX: (925) 258-0591 ·



Summer 2024 Newsletter Topics

- *Fraud Alert: Your Guide to Protecting Yourself in a Changing World*
- *10 Habits of Financially Successful People*
- *Osaic Wealth, Inc. Transition*

10 Habits of Financially Successful People

Just like an annual checkup keeps you physically well, considering the following items each year can help keep you financially healthy, too.

ONE Max out your year – The IRS sets maximum annual limits for contributions to your 401(k), IRA, health-savings accounts, and flexible-spending accounts.

Fraud Alert: Your Guide to Protecting Yourself in a Changing World¹

Financial fraud is an issue that impacts all of us.

KNOWLEDGE IS POWER. The good news, however, is that knowledge is power. The more we understand financial fraud and the common ways it's carried out, the easier it may be to avoid. This guide will provide an overview of several common scams, what to watch out for, and insights on how to protect yourself.

FRAUD IS COMMON. Sadly, financial fraud is a big issue. The monetary estimates vary wildly but are thought to be in the billions. Fraud can take a significant toll. Falling victim to fraud can have a severe emotional, and even physical, impact on victims. And with elder fraud, seniors often have no way to recoup the losses they suffer.

IT'S ALSO ON THE RISE. Data breaches happen more than we may ever know, exposing billions of records each year. Hackers target businesses -- big and small -- across a wide range of industries, from social media accounts to ride sharing services, and even healthcare companies. When you look at the millions of people impacted, it's no surprise that reports of identity theft are on the rise.

FRAUD OFTEN GOES UNREPORTED. Even though fraud is so common, it may still be significantly underreported.

1.9M

APRIA HEALTHCARE DATA
BREACH, MAY 2023

1.9 million customers had
personal data potentially exposed²

So why wouldn't someone seek help? There are many possible reasons:

- Embarrassment
- Doubt
- Dementia
- Involves a family member
- Fear of retaliation
- Don't know who to contact

This means we need to be proactive in talking to people about fraud. Give us a call and don't be afraid to ask questions. If you think someone you know might be a victim, let them know you can help.

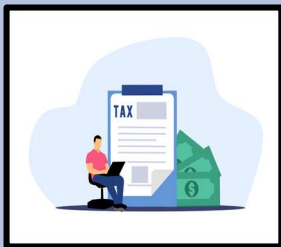
\$10.3B

ONLINE SCAMS AND LOSSES RISING

Over 800,000 cyber crime complaints
in 2022 with losses of \$10.3 billion³

In many cases, the more you contribute to these accounts, the more you build up your savings and investments while lowering your taxable income for the year. (See IRS TABLE on page 5 for 2024 limits)

TWO Help minimize your tax bill – Before year-end, evaluate your portfolio’s winners and losers for tax-loss harvesting opportunities. This is the process of offsetting assets that have increased in value (capital gains), which could increase your tax bill, with assets that have decreased in value (capital losses).



THREE Use it before you lose it – Some accounts, such as flexible-spending accounts (for both childcare or healthcare expenses), have cutoff dates. Remaining funds in these accounts can’t be applied to expenses next year, so make sure to stay caught up on receipts and reimbursements, or plan out purchases

HOW TO SPOT SCAMS

When it comes to fraud, the more you know, the better off you are. Here are some common scams, as identified by the U.S. government.*

Imposter Scams (charity, debt, prize)

Scammers pretend to be someone you trust, like a government employee or charity. The scam may relate to collecting a debt or winning a prize.

Know The Facts

- Caller ID can be faked
- Don’t provide any personal financial information
- You’ll never win a contest you didn’t enter

Imposter Scams (grandparent) Scammers call claiming to be a grandchild in trouble or a police officer, lawyer, doctor, etc. calling on their behalf. They may urge you not to contact the parents and ask for money.

Know The Facts

- Talk to your grandchildren about this scam
- Come up with an emergency code word
- Let them know you will always call their mom or dad

Mail fraud scams Any fraud that uses the U.S. Mail® is mail fraud. It could be relating to employment, telemarketing, veterans, finances, prizes, etc. and may originate online, over the phone, or by mail.

Know The Facts

- See common mail fraud schemes at usps.com
- Don’t share any financial information
- If you’re a victim, file a complaint at 1-800-372-8347 or uspis.gov/report

Money transfer/mortgage fraud Be wary of people you don’t know asking you to send money. Mortgage fraud targets homebuyers with complex schemes that appear legitimate.

Know The Facts

- Never send money to someone you don’t know
- Don’t email financial information
- Never follow instructions contained in an email before verifying them with trusted individuals

Romance scams Criminals adopt a fake online identity to gain a victim’s affection and trust. They establish a relationship as quickly as possible and make plans to meet that never happen.

Know The Facts

- Be careful what you make public online
- Go slowly and ask lots of questions
- Be wary if an individual seems too perfect
- If you haven’t met in person after a few months, you should be suspicious

Money mule scams A mule moves money that came from fraud victims. May be recruited through online job or social media posts, or by helping a love interest they met online or over the phone.

Know The Facts

- Being a money mule can lead to jail time
- Don’t send money or packages for people you don’t know
- Don’t open bank or crypto accounts for others
- Report scams at reportfraud.ftc.gov

TECHNOLOGY: HOW TO PROTECT YOURSELF

There’s no denying that modern technology brings countless benefits to today’s world. On the flip side, it also creates certain vulnerabilities. The first step is to be aware of any potential issues, then decide what personal approach works best for you.

SMART PHONES

Privacy Settings⁴ If you’ve ever wondered about the level of privacy you have on your cell phone or tablet, you’re not alone.

- Before installing an app, know what it can access, review the permissions, and use official app stores.
- If you already have an app, review the permissions, don’t sign in via social media, keep it updated and delete if not using.

Location Services⁵ This technology identifies the user’s physical and geographical location, which is then used to provide information, entertainment, or security.

- It’s based on access you allow on your phone and/or apps, and can be used to locate stores, get traffic updates, weather reports, ridesharing services, etc.
- The biggest disadvantage is the privacy concern in the event of a data breach. Some people prefer to limit app location services to when they’re using the app or turn it off on their device.

Social Media Despite the conspiracy theories, social media companies learn about you based

before the end of the year.

FOUR Rebalance – As different asset classes moved throughout the year, your portfolio’s intended asset mix likely shifted. At least once a year, consider rebalancing your portfolio to your goal allocations. Your financial professional can do this for you, or some accounts may allow you to opt in to automatically rebalance at a frequency of your choosing (e.g., quarterly, semiannually, annually).



FIVE Give unto others – Another important year-end task is to tabulate your charitable giving for the year. The IRS allows taxpayers to list charitable giving as itemized deductions, but any donations must be made before December 31 of the intended tax year.

on what you do in their apps and websites.⁶

- Virtual assistant apps like Siri or “Hey Google” are essentially verbal search engines that collect your data for marketing purposes. If you’re concerned about privacy, you can disable them, and choose to limit permissions to apps that ask for microphone access.⁷
- TikTok, the largest social app with about 150 million users, is Chinese-owned and required by Chinese law to give the government access to collected data such as facial ID, voice prints, texts, locations, and photos. It can also collect your data if you click on a video linked to TikTok.⁸
- Use diligence when using social media marketplaces to buy goods. Be aware of scams and always be diligent on where you meet the other party to stay safe.
- Be careful of online dating apps and the possible scams. Common sense goes a long way, but never provide money to someone on a dating app.

TIP: DON'T PUT IMPORTANT PERSONAL INFORMATION, SUCH AS YOUR ADDRESS OR THAT YOU'RE AWAY ON VACATION, ON SOCIAL MEDIA.

ARTIFICIAL INTELLIGENCE

A New Frontier⁹ According to IBM, at its simplest form, artificial intelligence (AI) is a field that combines computer science and robust datasets to enable problem-solving. Over the years, it’s gone through many cycles of hype, but the release of OpenAI’s ChatGPT seems to mark a turning point, particularly in natural language processing. But the generative models can also learn software code, molecules, natural images, and a variety of other data types.

The applications for this technology are growing every day, and we’re just starting to explore the possibilities. Examples include speech recognition, customer service, computer vision, recommendation engines, and automated stock trading.

Deepfakes¹⁰ But as the hype around the use of AI in business takes off, conversations around ethics become critically important. AI generated deepfakes are becoming more common. Deepfakes are a specific kind of synthetic media where a person in an image or video is swapped with another person’s likeness. Or, it could be

audio, with someone pretending to be someone you know.

Artificial intelligence is quickly getting better at mimicking reality, raising big questions over how to regulate it to avoid misuse like political propaganda or the creation of fake history. Countermeasures do exist, like software that can detect AI output, and AI tools that watermark the images or text they produce.

But there’s no universal standard yet for identifying real or fake content. For now, the best way to move forward is to be skeptical, do some fact checking, and to do your best to determine if what you’re seeing can be corroborated.

CRYPTOCURRENCY

Outpacing Regulation Cryptocurrency developments continue to outpace formal regulation. In 2022, the president issued an executive order “on Ensuring Responsible Development of Digital Assets.” These new recommendations attempt to create a federal framework that addresses market integrity and consumer protection.¹¹

Crypto Scams In addition to the complex nature and lack of regulation in cryptocurrency, consumers should also be aware of common scams involving cryptocurrency. The first is simply fraudulent activity by bad actors, such as the case with FTX, a trading venture focused on digital assets that grew into a sprawling crypto empire, then collapsed because of improperly diverted assets by chief executive Sam Bankman-Fried.¹²

But the fact is, consumers tend to know very little when it comes to how digital currency works or how to keep their digital assets safe. And since cryptocurrency payments do not come with any legal protections or government assurances, crypto scams are especially attractive for thieves. There’s also no centralized authority to flag suspicious crypto transactions, and all crypto transfers are irreversible. It’s easy to see why the industry is ripe for fraud.¹³

Other cryptocurrency scams mirror some scams we’ve already discussed, but try to get cryptocurrency as the payment. According to the Federal Trade Commission (FTC), more than 46,000 people reported losing over \$1 billion in crypto to various scams from January 2021 through June of 2022. And that figure only includes people who willingly shared the information with authorities.¹³

SIX Take a step back
– A lot can happen in a year. Did you get married, divorced, or have a child? Major life events such as these can play a major role in your finances, so make sure your financial and tax professionals know about them. It's also a good time to make sure your beneficiary information—on all accounts and policies—is up to date.

SEVEN Stay covered
– In addition to reviewing health, vision, and dental coverage during annual enrollment, consider your other insurance needs as well. Whether it's home, auto, or life insurance, make sure you have adequate coverage. You may also want to consider shopping around to make sure you're not overpaying or under-covered.

EIGHT Where do things stand?
– Evaluate your contributions and budget for the previous year. Did you have any budget surpluses that you can reallocate to investments, savings, or lowering debt? Then look ahead: Are you factoring in changing expenses, such as resuming student-loan

TIP: AS WITH OTHER SCAMS, JUST WATCH OUT FOR ANYTHING THAT SEEMS TOO GOOD TO BE TRUE, “PAY TO PLAY” JOB POSTINGS, PROMISES OF GUARANTEED RETURNS, AND UNEXPECTED COMMUNICATIONS REGARDING CRYPTO.

TAKE ACTION

Online One way to protect your identity is to create online accounts for every financial or medical institution you work with. You may think that you're keeping yourself safe by not creating an online account, but you may be surprised to learn that the opposite is actually true. If you don't create an online account, someone else potentially can.

- Create online accounts and monitor them regularly.
- Use strong passwords, don't reuse them, and consider a password manager.
- Enable multi-factor authentication when available.
- Use auto-pay instead of sending a check in the mail.
- Don't overshare on social media (and tell your kids not to either).

Debit & Credit Cards Not surprisingly, credit cards are a common target in financial abuse or exploitation. It could be a situation like phishing, where a thief steals credit card information. In other cases, a trusted person may get possession of a credit card and be tempted to use it for him or herself. Simple steps can reduce the risk of debit or credit card fraud.

- Don't use debit cards to make purchases and never give out your PIN. If compromised, the scammer has access to your bank account, similar to personal checks.
- Consider using a credit card with a low limit (\$1,000 or \$1,500) for day-to-day purchases like groceries, gas, or online purchases. Carefully review credit card statements for fraud. Watch out for things like magazine subscriptions and recurring charitable gifts, which could be a fraudulent income stream.

Electronic Devices Protect the physical devices that allow you to go online by taking the following action steps:

- Install anti-virus and anti-spyware software and keep them updated.
- Avoid phishing emails by not opening files or photos, clicking on links, or downloading programs sent by strangers. It could expose your system to a virus or spyware.
- Don't send personal information over your laptop or smartphone, especially on a public wireless network, like in a coffee shop or airport. They're not secure.
- Keep financial information on your devices only when necessary. Don't use an automatic login feature and log off when finished in case of theft. Safely dispose of data before replacing devices.
- Set up a security question, or a PIN with your cell phone provider. Otherwise, hackers can port your number and steal thousands of dollars from important accounts in a matter of days.

Identity Theft If you believe you've been the victim of identity theft, or if your personal information has been lost or exposed, identitytheft.gov (in Spanish at robodeidentidad.gov) is the government's free, one-stop resource for reporting and recovering from identity theft.

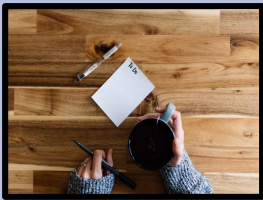
- Visit the site to get a personalized, interactive recovery plan.
- Follow the steps provided in your recovery plan, which may include prefilled letters, affidavits, and forms, follow-up reminders, advice for specific breaches, and plans for more than 30 types of ID theft.



Credit Bureaus Equifax, Experian, and Transunion collect information about where you live and work, how you pay your bills,

payments, for next year?

NINE Simplify – If you changed jobs and left your old retirement account behind, it may make sense to roll over any old accounts and consolidate them under one provider. The same is true for debt: If you have credit-card debt, consider transferring the balance for a lower rate to reduce your payments.



TEN Prepare for next year – If you haven't been in touch with your financial professional, now may be a good time to schedule a financial-wellness checkup. It's a great time to step back, acknowledge what you've achieved so far, and set your goals for the coming year.

whether you have been sued, arrested, or filed for bankruptcy. All of this information is combined in a credit report. The credit bureaus will sell your credit report to creditors, employers, insurers, and others. Those companies will then use the credit reports to make decisions about extending credit, jobs, and insurance policies to you.

- Find out how to obtain your credit report, make corrections, and more at usa.gov/credit-reports.
- Get information on fraud alerts and credit freezes at consumer.ftc.gov

Offline Even with so much of our lives being managed online these days, there are still risks associated “offline” as well. Mainly, you want to be careful with your mail and shred all documents with personally identifiable information before throwing them away or recycling them.

- Opt for e-delivery when possible to avoid sensitive material being mailed to you.
- Retrieve mail as quickly as possible to avoid theft.
- Place a hold on mail while on vacation.
- Have new checks mailed to your bank or other secure location.
- Shred all documents with personally identifiable information.

Social Security Number Your Social Security number is a coveted piece of information for criminals. Keep a close hold on it and ask questions before sharing it, including if you can use a different kind of identification. If someone asks you to share your number or your child's number, ask:

- Why it's needed
- How it will be used
- How it will be protected
- What happens if you don't share the number

IF YOU THINK YOU'RE THE TARGET OF A SCAM

There are a number of steps you can take to protect yourself. First, be alert to financial fraud. Awareness is perhaps our most effective tool to fight scammers. Second, if you suspect you've been defrauded, talk with someone you trust. Whether it's a spouse, adult child, attorney, tax advisor, or your financial professional, simply talking to someone about the situation can be helpful in determining whether fraud has occurred.

If you think it's a scam, you can call local law enforcement, your state attorney general, or the national credit bureau. Identifythefth.gov can also be a valuable resource to help create a recovery plan.

Osaic Wealth, Inc.

Securities America, the firm I use to support my business operations, announced last June that their parent company (formerly Advisor Group) adopted the new brand and name of Osaic – a play on the word Mosaic that reflects the firm's history and heritage while also keeping true to the firm's commitment to investors. Securities America will transition to Osaic (Osaic Wealth, Inc.) in June of this year.

The name change represents Osaic's mission to transform wealth management in a lasting way, guided by the belief that as your Financial Professional, I can have a powerful impact on your life and those of your family and future generations.

You may notice the new name and logo on materials from the firm, but otherwise, you will not experience any changes.

Systems and forms are being updated to reflect this new name, but you may continue to see the Securities America or Advisor Group name until that is completed.

Osaic will provide you with an official notification of the upcoming change. There will be no action required of you as a result of the notification.

My commitment to you and your financial goals remains stronger than ever. This change will not impact the way we work together, and I'll continue to manage your accounts in the same way as today.

IRS Contribution Limits

	2024
Retirement Plans: 401(k), 403(b), 457	
Defined contribution limit (your contributions plus employee matches/contributions)	\$69,000
Elective deferral limit (your contributions)	\$23,000
Catch-up contribution limit (age 50+)	\$7,500
Traditional and Roth IRAs	
Annual contribution limit	\$7,000
Catch-up contribution limit (age 50+)	\$1,000
Health Savings Accounts	
Annual contribution limit for individual	\$4,150
Annual contribution limit for family	\$8,300
Flexible savings accounts	\$3,200
Dependent Care Flexible Savings Arrangements	
Married filing jointly	\$5,000
Married filing separately	\$2,500

Source: IRS

**Park Place Wealth
Advisors, Inc.**

Daniel J Gannett

18 Orinda Way
Orinda, CA 94563
(925) 254-7766
(408) 733-0245
Fax (925) 258-0591

As always, we encourage investing with your goals in mind, keeping a reserve for emergency needs.

We are available for in person, phone or zoom reviews. Give the office a ring and we can discuss your investing goals and needs.

Estate Planning

Retirement Planning

*Long Term Care
Planning*

Insurance

*Corporate Qualified
and Non-Qualified
Retirement Plans
-401(k)-*

*Educational Funding
-529 Plans-*

Charitable Planning

Content courtesy of

¹Transamerica – Financial Fraud Field Guide – Your Guide to Protecting Yourself in a Changing World
https://cdn.bfldr.com/86JM1UOD/as/6v4rbxbq6bgmnw3jkf4n332f/Financial_Fraud_Field_Guide_-_Your_Guide_to_Protecting_Yourself_in_a_Changing_World

² “Data Breaches That Have Happened in 2022 and 2023 So Far,” Tech.co, June 2023

³ “FBI Internet Crime Report,” Internet Crime Complaint Center, July 2023

*“What Are Some Common Types of Scams?” Consumer Financial Protection Bureau, April 2023

⁴ “How to Protect Your Privacy on Apps,” Federal Trade Commission, accessed July 2023

⁵ “Location-Based Services: Definition and Examples,” Business News Daily, March 2023

⁶ “Here’s How Facebook is Actually Listening to You,” Komando.com, May 2022

⁷ “Is My Phone Listening to Me? Yes, Here’s Why and How to Stop It,” Norton, June 2023

⁸ “TikTok’s Dark Side: Why It’s More Than Just a Fun App and You Need to Remove It,” Komando.com, March 2023

⁹ “What is Artificial Intelligence (AI)?” IBM.com, accessed September 2023

¹⁰ “AI-Generated Deepfakes Are Moving Fast. Policymakers Can’t Keep Up,” NPR, April 2023

¹¹ “U.S. Treasury Encourages New Laws to Address Crypto Regulation Gaps,” Reuters, October 2022

¹² “The Crypto Fraud Case Against Sam Bankman-Fried and FTX,” The Washington Post, September 2023 ¹³

“What Are The Most Popular Crypto Scams to Watch for in 2023,” TIMEstamped, May 2023

Hartford Funds – 10 Habits of Financially Successful People <https://www.hartfordfunds.com/practice-management/client-conversations/financial-planning/10-habits-of--financially-successful-people.html>

IMPORTANT DISCLOSURES

PARK PLACE WEALTH ADVISORS, INC. A REGISTERED INVESTMENT ADVISOR.

DANIEL J GANNETT CA INSURANCE LICENSE OF27019

SECURITIES OFFERED THROUGH **OSAIC WEALTH, INC.**, MEMBER FINRA/SIPC, AN INDEPENDENT BROKER/DEALER. **OSAIC WEALTH, INC.**, AND PARK PLACE WEALTH ADVISORS, INC. ARE NOT AFFILIATED ENTITIES.

OSAIC WEALTH, INC. DOES NOT PROVIDE TAX ADVICE.

THESE MATERIALS ARE PROVIDED FOR GENERAL INFORMATION AND EDUCATIONAL PURPOSES BASED UPON PUBLICLY AVAILABLE INFORMATION FROM SOURCES BELIEVED TO BE RELIABLE – WE CANNOT ASSURE THE ACCURACY OR COMPLETENESS OF THESE MATERIALS. THE INFORMATION IN THESE MATERIALS MAY CHANGE AT ANY TIME AND WITHOUT NOTICE.

IF YOU ARE A REGISTERED INVESTMENT ADVISORY CLIENT, WE ARE REQUIRED TO ANNUALLY OFFER TO DELIVER TO YOU, FREE OF CHARGE, OUR BROCHURE, OR OUR MOST RECENT FORM ADV 2A AND 2B IN PAPER OR ELECTRONIC FORMAT, WHICH DETAILS THE BACKGROUND, BUSINESS PRACTICES, AND PHILOSOPHY OF THE FIRM AND ITS AFFILIATES. SINCE THE LAST ANNUAL AMENDMENT TO THIS BROCHURE WAS FILED IN FEBRUARY 2024 NO MATERIAL CHANGES WERE MADE TO THIS DISCLOSURE BROCHURE. WE WILL ENSURE THAT YOU RECEIVE A SUMMARY OF ANY MATERIAL CHANGES TO THIS AND SUBSEQUENT DISCLOSURE BROCHURE WITHIN 120 DAYS AFTER OUR FIRM’S FINANCIAL YEAR ENDS. OUR FIRM’S FISCAL YEAR ENDS ON DECEMBER 31, SO YOU WILL RECEIVE THE SUMMARY OF MATERIAL CHANGES NO LATER THAN APRIL 30 EACH YEAR. AT THAT TIME, WE WILL ALSO OFFER OR PROVIDE A COPY OF THE MOST CURRENT DISCLOSURE BROCHURE. WE MAY ALSO PROVIDE OTHER ONGOING DISCLOSURE INFORMATION ABOUT MATERIAL CHANGES AS NECESSARY

IF AT ANY TIME YOU WOULD LIKE A COPY OF THE MOST RECENT DISCLOSURE BROCHURE OR OUR PRIVACY POLICY, PLEASE CONTACT US VIA EMAIL, PHONE, FAX OR LETTER AND WE WOULD BE HAPPY TO SEND YOU A COPY OF THE MOST CURRENT DOCUMENT. WE WILL ALSO PROVIDE OTHER ONGOING DISCLOSURE INFORMATION ABOUT MATERIAL CHANGES AS REQUIRED.