Gibson Capital, LLC
Registered Investment Adviser

PRINTER-FRIENDLY CYBERSECURITY CHECKLIST

☑ TIP #1: EDUCATE YOURSELF AND STAY CAUTIOUS

- ☐ Learn to identify phishing emails. The following clues may help alert you that you have received a scam communication:
  - ·It is unexpected. Often the sender's email address is a giveaway (such as amazn.com instead of amazon.com).
  - ·It tries to compel you to take action, potentially using language intended to create fear or a sense of urgency.
  - ·It contains jumbled, misspelled, or incorrect words, syntax, or grammar.
  - ·The sender's phone number does not match the company's published list of numbers on their website.
  - ·The links or logos in the message look off or are slightly different from a company's official link or logo.
- ☐ Always be suspicious of unsolicited emails or calls that ask you to take action, especially if they suggest that immediate action is required.
- ☐ Be wary of tax scams. Remember that the IRS will not initiate contact with you by phone, email, or social media. They will never ask for personal financial information by email.
- ☐ Text messages, phone calls, or emails that say "We're contacting you about fraud" are typically a red flag.
- ☐ If you think a message may be legitimate but you're not positive, contact the company independently through an official channel, such as a phone number listed on its website.
- ☐ Be aware that cybercriminals can easily fake incoming phone numbers to make it appear that they are calling from a trusted institution like your bank, brokerage firm, government agency, or utility company.
- ☐ Look out for suspicious texts sent as a group text. Fraudsters can set the name of a group text so that it appears to come from a trustworthy company name.
- ☐ Never click links or attachment files in an email from an unexpected source, which may contain malware intended to infect your computer.
- ☐ Cybercriminals often ask for login credentials and personally identifiable information like your Social Security Number, and they may ask you to read back security codes or passwords that are texted to you. Never share this information with an unverified inbound caller.
- ☐ Limit the personal and work-related information that you share on social media. Cybercriminals can use this information to impersonate you or people you know in an attempt to defraud you.
- ☐ If someone reaches out to you on WhatsApp or another chat messaging platform to offer you investment advice, just delete the message! Although legitimate financial companies are increasingly utilizing WhatsApp for marketing purposes, openly soliciting business or offering specialized investment advice to "exclusive" investment groups has become a common and costly investment scam, leading to millions of dollars stolen from trusting investors looking for hot stock tips.
- ☐ Never give an unverified individual remote access to your computer after receiving a call, email, or pop-up request to do so.

☑ TIP #2: PROTECT YOUR INVESTMENT ACCOUNTS

- ☐ When you open an account with a new institution, establish online access for the account and create a unique User ID that is different from your Social Security Number.
- ☐ Regularly review your address, phone number, email addresses, and beneficiaries on file for your accounts and proactively update them when needed. Make sure that the institutions that you work with know how to reach you if they need to.
- ☐ Consider enrolling in electronic statement delivery to reduce the possibility of mail theft. Your paper statements and tax forms contain sensitive information that fraudsters can use to gain access to your accounts, especially if you have multiple homes or travel often.
- ☐ Enable Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) for your accounts. Always use a secondary verification method like a text code or app to log in.
- ☐ Create complex passwords. Use long, unique passphrases for each account to prevent unauthorized access, and don't use the same password for multiple accounts.
- ☐ Activate account alerts if the custodian offers them. Set up notifications for withdrawals, password changes, address changes, or trades to quickly spot fraud.
- ☐ Use biometrics when possible to log in to your accounts. Many custodians now utilize fingerprints, facial recognition, or voice recognition for mobile apps, and they generally offer better protection than passwords.
- ☐ Monitor your account transactions and statements regularly, even if you are not trading. The customer fraud protection guarantees for many custodians, like Fidelity, require account holders to report fraudulent activity within 30 days in order to be reimbursed, so it is crucial that you check your account history frequently.
- ☐ If you are working with any other investment advisors, make sure that they review client activity daily and verbally confirm all third-party disbursement requests to ensure that the requests are legitimate. (We do!)
- ☐ Avoid accessing your financial accounts from public computers in libraries, cafes, airports, or other locations when you cannot use your own device.

TIP #3: SECURE YOUR DEVICES AND NETWORK

- [ ] Install antivirus and personal firewall software.
- [ ] Apply operating system updates and antivirus patches as soon as they are released. Configure your software to allow auto-updates so that fixes can automatically be applied when new vulnerabilities are discovered.
- [ ] Change all default passwords that come with your devices, including smart home technology.
- [ ] Do not save passwords in your web browser, as they are susceptible to malware attacks.
- [ ] Consider using a password manager program like LastPass, Dashlane, or 1Password, which can make it easy for you to use strong credentials for your financial accounts.
- [ ] Secure your home Wi-Fi network with a strong password and monitor the devices that connect to it (some service providers even offer tools and alerts to make this easy).
- [ ] Contact your home internet provider and ask if they offer a Virtual Private Network (VPN) for residential customers. VPNs encrypt your internet connection and mask your public IP address, providing a layer of privacy and security.
- [ ] Exercise caution when connecting to the internet via unsecured or unknown wireless networks, such as those in public locations like hotels, cafes, or airports. These networks may lack virus protection, are highly susceptible to attacks, and should never be used to access confidential personal data.
- [ ] Only download apps from a reputable provider like the Apple App Store rather than the internet.
- [ ] Consider using a dedicated iPad or tablet for online shopping to segment riskier activity from a device where financial data like statements and tax forms are saved.
- [ ] In case devices are lost or stolen, activate security features such as passcodes, lock/auto-lock functions, remote lock/data wipe, “find my phone,” and face/touch ID.
- [ ] Before trading in an old device, erase any personal information it may contain by resetting the device to its factory settings.
- [ ] If criminals gain access to your phone calls, text messages, voicemails, or emails, they can potentially steal financial statements, personal information, or one-time passcodes—enabling them to break into your accounts.
- [ ] Here are several warning signs that your phone or email has been compromised:
  - ·You stop receiving phone calls, text messages, or email notifications.
  - ·Your phone says “no service” or “emergency calls only.”
  - ·Your cell or email provider notifies you of changes to your account.
  - ·Messages are being sent from your email or cell number that you did not originate.
- [ ] If you notice any of these warning signs, contact your cellphone or internet provider right away to see if your account has been compromised.

TIP #4: I THINK I'VE BEEN HACKED...NOW WHAT?

- [ ] If you realize that your phone or computer is actively being compromised, disconnect from the internet. Turn the Wi-Fi connection off or unplug the network cable to stop data from being sent to the hacker.

- [ ] **If you're a client of Gibson Capital's, call us as soon as possible** so that we can help you assess the scope of the breach, work with our custodians to lock down your accounts, and prescribe the best course of action for you based on guidance from our custodians and business partners.

- [ ] Contact your other financial institutions to report the breach. They may transfer you to their fraud department. Ask if it is possible to add restrictions to your accounts to prevent outbound distributions or transfers.

- [ ] Use reputable antivirus or malware software to scan your devices to identify and remove any potential spyware (or hire a qualified professional who can do it for you).

- [ ] Contact the three major credit bureaus to add a fraud alert or credit freeze to protect your financial reputation. A credit freeze stays in place until you lift it, offering the strongest long-term protection by preventing criminals from establishing new credit accounts in your name. Fraud alerts are ideal if you suspect fraud but need easier access to credit. Both options are free and should not prevent you from using your existing credit cards.

Equifax	Experian	TransUnion
800-525-6285	888-397-3742	800-680-7289

- [ ] If your Social Security Number has been stolen or someone has filed a fraudulent tax return in your name, you should report the fraud to both the Social Security Administration and the IRS to prevent criminals from stealing tax refunds, claiming benefits, or using your information for employment (or unemployment benefit) purposes.
  - ·Social Security Administration: 800-772-1213
  - ·Internal Revenue Service: 800-829-0433

- [ ] File an identity theft report with your local police department to document fraudulent use of your personal information. A report could be necessary as proof for creditors, so request a copy of the report for your records.

- [ ] Report the breach to the authorities by submitting details about the incident to the Federal Trade Commission (FTC) at IdentityTheft.gov.

- [ ] Notify your friends, family, and colleagues that you were hacked. Warn them not to click links or send money in response to messages from you.

- [ ] Monitor your credit reports regularly for any suspicious activity—such as profile changes, transaction attempts, or unfamiliar activity—they can help you detect suspicious events quickly.