Essential Risk Management Tips for CPAs

35 Valuable Lessons from CAMICO

CAMICO®

Introduction

Over the past 35-plus years, CAMICO has collected valuable insights and information from more than 8,700 CPA policyholder firms across the country and from our own jury experience, research and consultations with defense attorneys. Here are 35 valuable tips, as a way to help CPAs and their firms better manage professional and employment practices liability risk exposures. To learn more about each of these tips, visit the "Read More" links.

FRAUD, EMBEZZLEMENT & BANK RECONCILIATIONS

01

What is your job?

At the core of risk management insight is how the general public and juries view the CPA's job. Our experience tells us that the CPA's job is to advise of opportunity and warn of risk. And not just the client, but third parties as well, especially when financial statements are being issued.

Read More: Malpractice Risks Increase During Difficult Economic Times

02

"Limited services" does not mean "limited responsibility."

The CPA's responsibility is defined by: 1) the nature of the service, and 2) the length of time the CPA has provided the service. Five years of servicing a small business is enough for a jury to expect the CPA to have a profound understanding of the business, even if only tax returns and compilations were involved.

Read More: Embezzlement and the 'Classic' Claims Scenario

03

Embezzlements — don't miss the low-hanging fruit.

Embezzlement claims against CPAs are often the easiest to avoid, yet CPAs often miss red flags because they don't see embezzlement prevention as their job. Upon accepting the client, and biannually thereafter, send a short letter to all small business clients, explaining embezzlement risks and how to minimize them.

Watch: The CPA's Guide to Avoiding Embezzlement Fraud (Video)

04

Hindsight is perfect.

When everything and everybody is judged in hindsight, an embezzlement is always easier to spot. Unless the engagement is specifically intended to find fraud, CPAs should: a) make sure the client understands the CPA is not responsible for finding fraud, b) educate the client about embezzlement risk, c) emphasize the need for bank reconciliations, and d) instruct the owner to open all bank statements.

Read More: Advise and Warn Clients of Embezzlement Risks

05

Respect the "rec."

Many clients do not timely reconcile their bank statements. In hindsight, if an embezzlement occurs, this tardiness becomes a red flag of fraud that should have put the CPA on alert. Train staff to pay attention to bank reconciliation tardiness and defects, and to communicate these issues to the client.

Read More: Advise and Warn Clients of Embezzlement Risks

06

When fraud is suspected, act.

If fraud or misappropriation of assets is suspected, recommend in writing to the client that a fraud exam or forensic investigation under a separate engagement be conducted by a qualified professional. If the client declines, obtain the declination in writing.

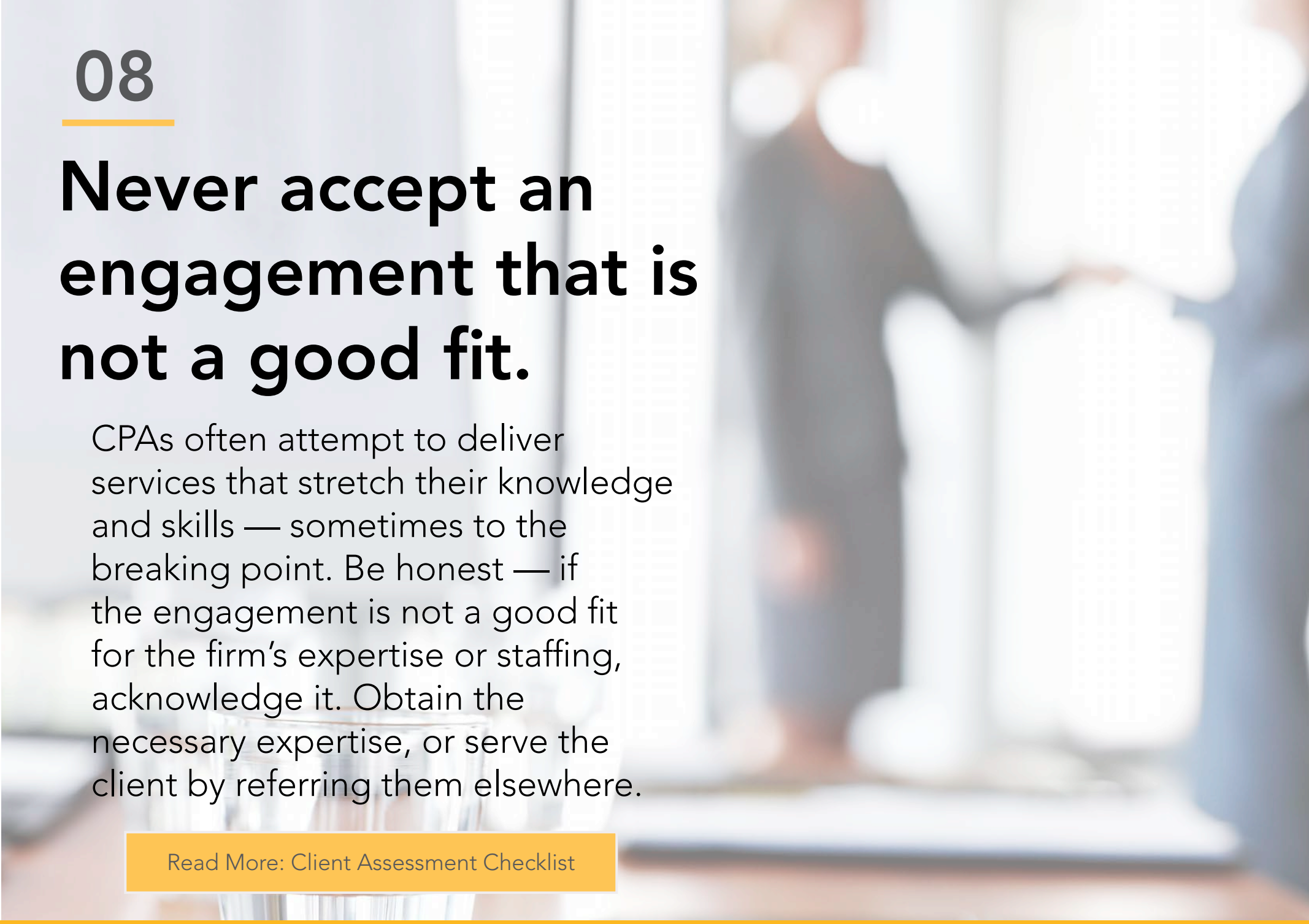
07

Have you got what it takes?

If the firm is controlling client funds and writing checks to pay client bills, take appropriate steps to safeguard the funds. Find out whether procedures are in place before accepting such engagements. Gain a detailed understanding and establish controls that will prevent the misuse of client funds.

Read More: Disappearing Client Funds

CLIENT SCREENING



08

Never accept an engagement that is not a good fit.

CPAs often attempt to deliver services that stretch their knowledge and skills — sometimes to the breaking point. Be honest — if the engagement is not a good fit for the firm's expertise or staffing, acknowledge it. Obtain the necessary expertise, or serve the client by referring them elsewhere.

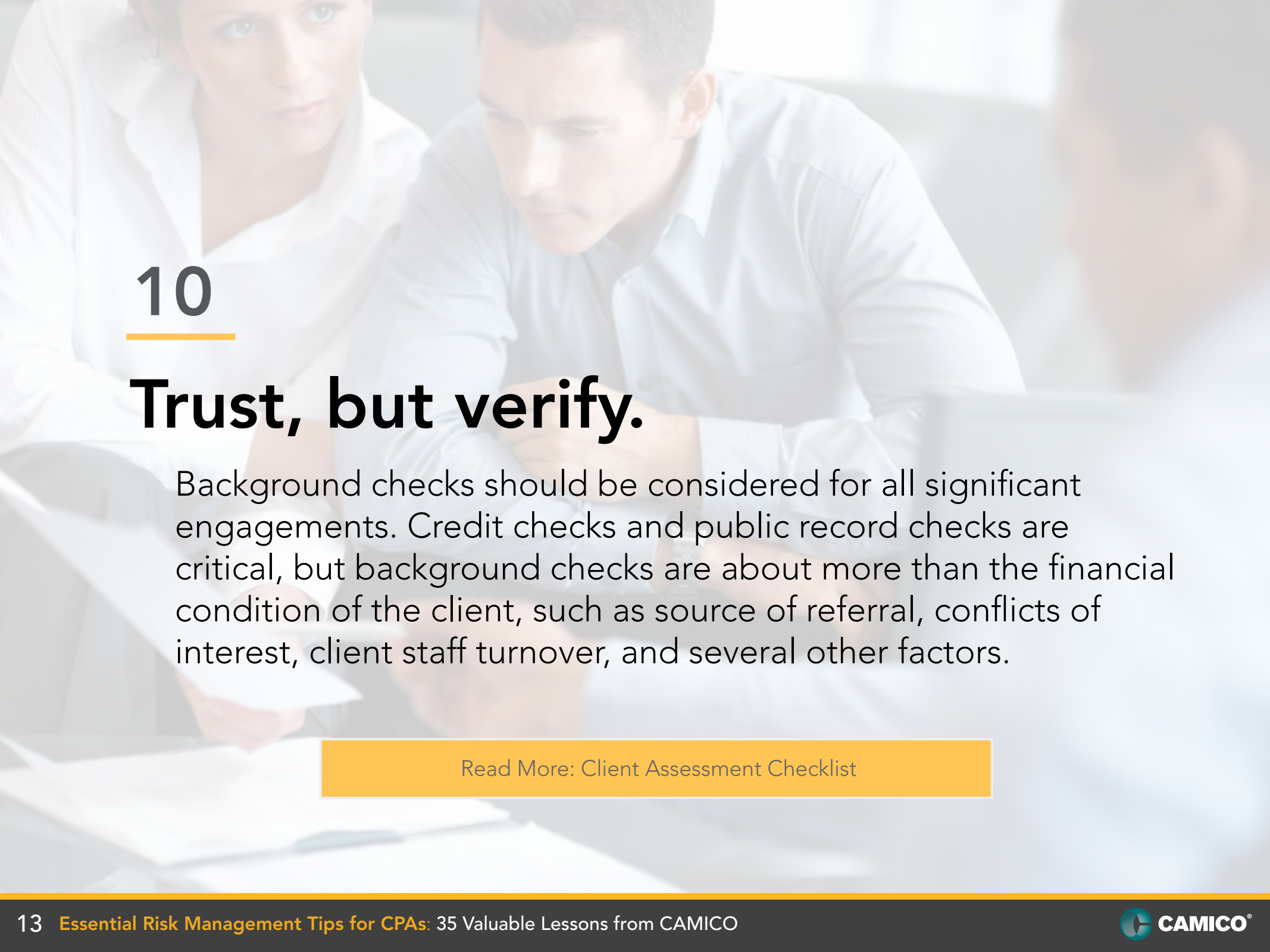
Read More: Client Assessment Checklist

09

Is this the kind of client you want?

Communicate with predecessor accountants and third parties to obtain as much information as possible about the client. If the client refuses to grant permission for these conversations, that's a red flag not to accept the client. For some engagements, CPAs will need to consider potential or actual conflicts of interest, and whether independence and objectivity are impaired in appearance or in fact.

Read More: Client Assessment Checklist



10

Trust, but verify.

Background checks should be considered for all significant engagements. Credit checks and public record checks are critical, but background checks are about more than the financial condition of the client, such as source of referral, conflicts of interest, client staff turnover, and several other factors.

Read More: Client Assessment Checklist

11

Address client-induced "heartburn."

Difficult client behavior such as slow payments, withheld information or documents, and unresponsiveness should be remedied, or the CPA may need to disengage. A red flag: when information appears to be deliberately withheld, and the CPA is urged by the client to proceed without it.

Read More: 5 Reasons to Disengage From a Tax Client

ENGAGEMENT LETTERS

12

Bridge the gap.

Use an engagement letter for every engagement: new engagements, repeat engagements, routine engagements, and especially with changed engagements. By clearly defining an engagement's purpose, services and limits (specifically what you will and won't do), you can avoid "the expectation gap."

Read More: Engagement Letter Do's and Don'ts

13 Proactively manage fee issues.

Disclose clearly to clients in the engagement letter how the firm is paid and what its arrangements are with third-party providers. Include billing and collection policies as well as stop-work provisions that can be enforced if payments are not received in accordance with the policies. Consider requiring a retainer.

Read More: Protect Your Business with Better Billing and Collection Practices

14 Don't assume that conflicts will never happen to you.

When used correctly in the right situations, mediation and arbitration are cost-effective and efficient options to litigation, though they're not always recommended. Confirm with your legal counsel and liability insurer the applicability of Alternative Dispute Resolution agreements in your state.

Read More: Alternative Dispute Resolution … When to Use Mediation and Arbitration

15

Knowing is better than suspecting.

Note any red flags in the client's background, wealth status and other information indicating they may have financial interests located in other countries. Be sure to include a question pertaining to FBAR and FATCA in the tax organizer, and make inquiries about information regarding other sources of income.

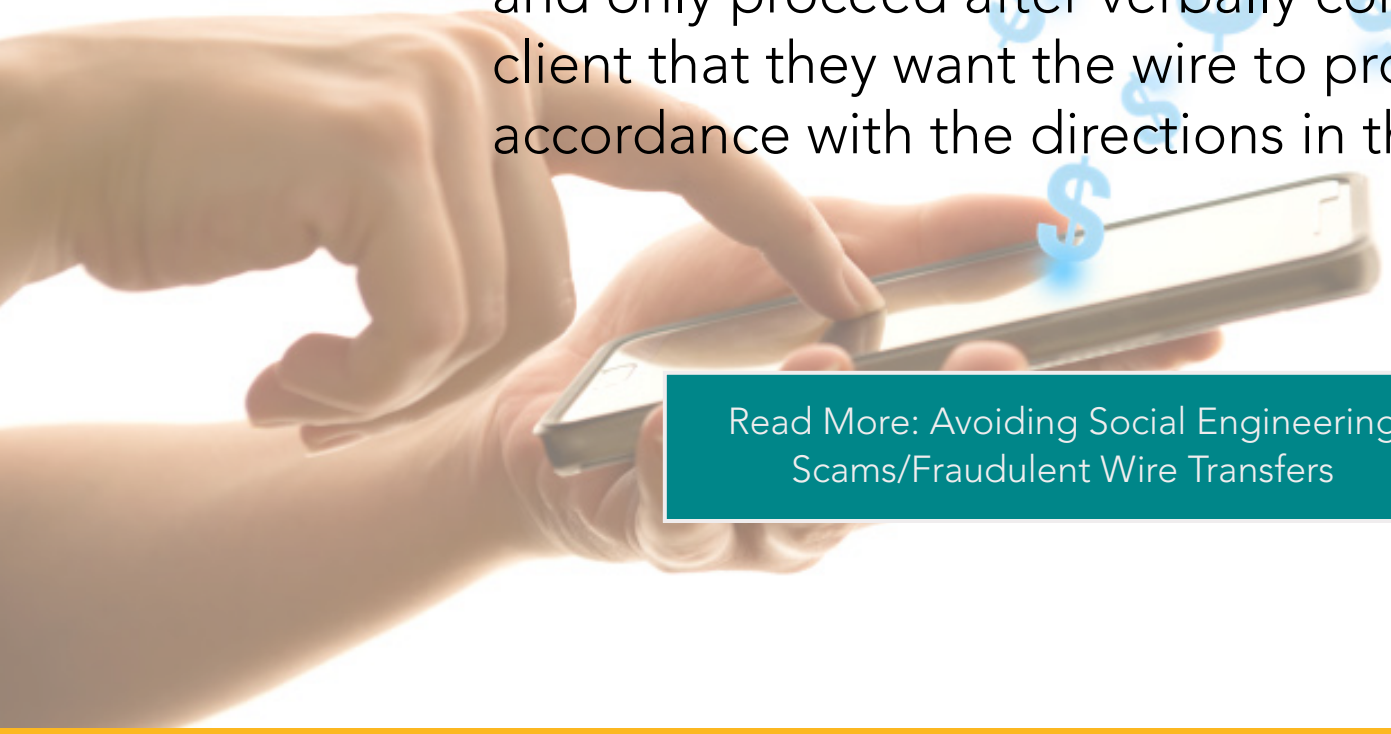
Read More: Taxpayer Filing Requirements for Foreign Accounts

CYBER

16

Be wary of any wire transfer requests.

In the era of cybercrime and email address spoofing, be wary of any wire transfer requests made via email and only proceed after verbally confirming with the client that they want the wire to proceed and in accordance with the directions in the email.



Read More: Avoiding Social Engineering Scams/Fraudulent Wire Transfers

17

Lock the doors to the castle.

Encrypt hard drives, electronic data, electronic files, and email. This will help protect: data in the event a computer or drive is lost or stolen, personally identifiable information, files and email attachments, and entire email messages, including the body of the message.

Read More: Test Your Cyber IQ

18

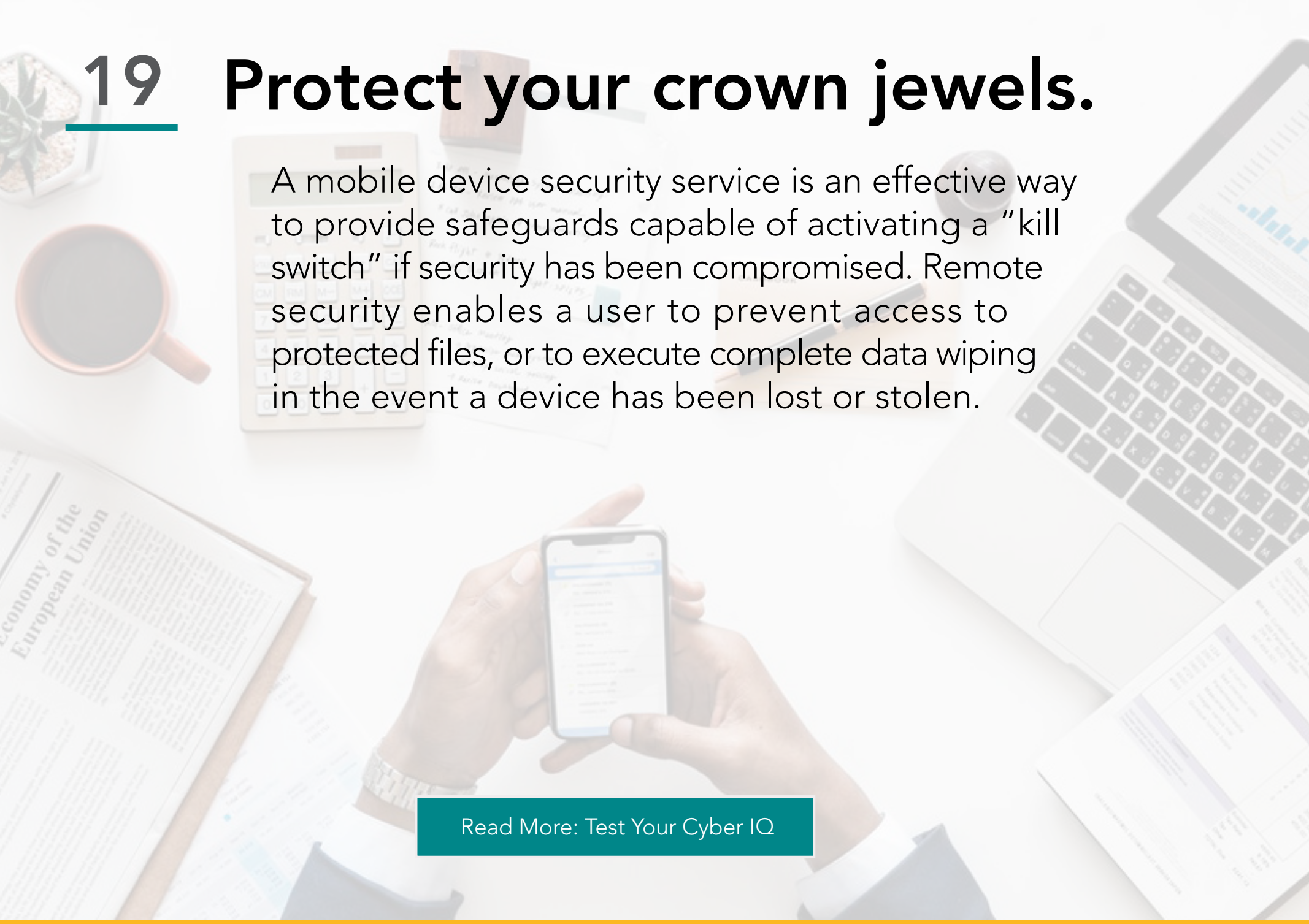
Back up data frequently.

Back up all important data and information frequently to reduce the likelihood that critical data is lost in the event of a cyberattack or physical incident such as a fire or flood. Protect the backups in a remote or external location where they are safe from ransomware that seeks out backup copies. Periodically, verify whether the backup is working.

Read More: Hacker Attacks on Email Systems and Tax Files

19 Protect your crown jewels.

A mobile device security service is an effective way to provide safeguards capable of activating a "kill switch" if security has been compromised. Remote security enables a user to prevent access to protected files, or to execute complete data wiping in the event a device has been lost or stolen.



Read More: Test Your Cyber IQ

20 Don't go from "hero" to "zero."

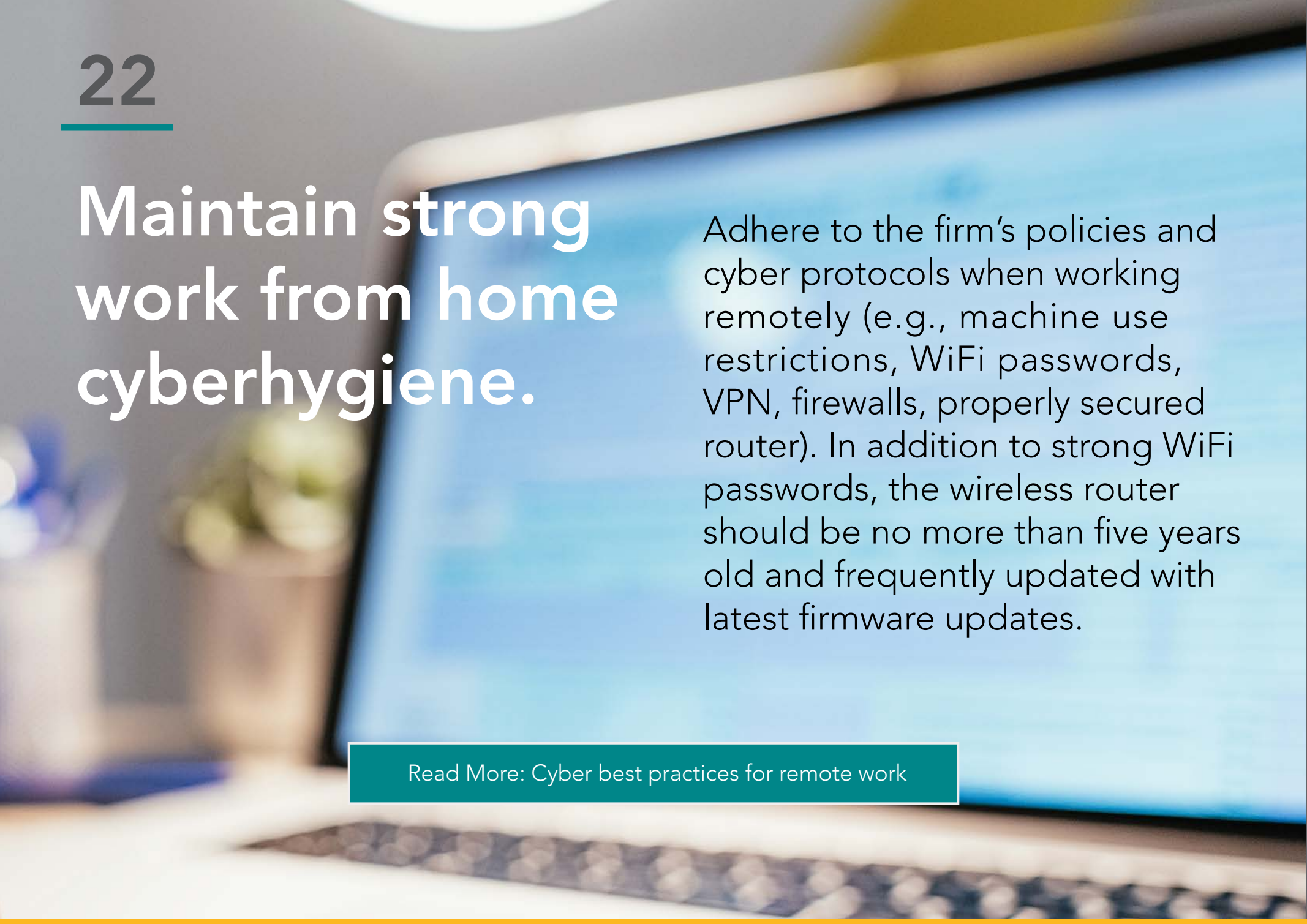
Educate all employees about good cyber hygiene and how to avoid phishing attempts that target them with social engineering techniques designed to install malware or to deceive and elicit confidential information. Many thefts occur when someone clicks a link, pop-up or attachment that contains malware. Some malware downloads secretly into computers and allows thieves to covertly capture each keystroke or gain remote access to the computer, allowing them to steal the data stored there.

Read More: Hacker Attacks on Email Systems and Tax Files

21 Prioritize cybersecurity awareness training.

Even the best employees can become complacent about adhering to cybersecurity best practices when working remotely. To better manage remote access threats, set clear rules to govern how employees work remotely. Employees are the first line of defense against most, if not all, cybersecurity attacks. Special attention should be given to ensure that your firm continues to prioritize appropriate firm-wide cybersecurity awareness training.

Read More: Cyber best practices for remote work



22

Maintain strong work from home cyberhygiene.

Adhere to the firm's policies and cyber protocols when working remotely (e.g., machine use restrictions, WiFi passwords, VPN, firewalls, properly secured router). In addition to strong WiFi passwords, the wireless router should be no more than five years old and frequently updated with latest firmware updates.

Read More: Cyber best practices for remote work

23

Know how cyber risk exposures impact the firm as well as the client.

Cyber exposures and coverages are divided along two lines: **1)** first-party, which refers to losses directly borne by the insured firm, and **2)** third-party, which refers to damages alleged by clients or other third parties for which the firm may be liable. The line between the two may become blurred when a hacker has managed to penetrate both the firm's and client's computer systems. But insurance coverages typically respond according to which party is bearing losses or alleging damages and why it's important to know all the facts.

Read More: Understanding First-Party and Third Party Cyber Coverages

GENERAL RISK MANAGEMENT

24 Don't admit liability or assume damages.

Avoid admitting liability or assuming damages under the contract/engagement with the client or other parties. Doing so could exclude the claim from coverage under the professional liability policy, and it increases risk. Avoid agreements that include hold harmless or indemnification provisions.

Read More: Indemnification: Understanding Your Risks

25

CPA-to-lender letters: Don’t put yourself at risk.

Before responding to third-party requests from lenders: a) receive written consent from the client before disclosing tax return information, b) document only facts and the services you performed, c) refrain from speculating on future events and avoid making conclusions not supported by the services performed by the client.

Read More: CPA-to-Lender ‘Comfort Letters’

26

Report potential claims, errors and omissions.

Early notification of a potential error will help claims specialists assist in mitigating the impact of the error. Early notification may also comply with the reporting requirements of the policy, helping preserve coverage if a claim is later asserted. CAMICO policyholders may benefit in a variety of ways from early reporting. For example, a 50% reduction in the deductible, up to $50,000, for early reporting of a potential claim during the policy period in which it becomes known or use of formal mediation to attempt to resolve a claim.

Read More: Report Potential Claims and Claims as Early as Possible

27

Consult an attorney before accepting a trusteeship.

Consult with an attorney or risk adviser who specializes in trusts before accepting a trustee or executor engagement, particularly if the firm does not frequently perform this service. Trustee and executor engagements are often high risk, and CPAs should become informed before accepting them.

Read More: Trustee Red Flags and Best Practices

28 Contact a professional liability risk adviser or attorney before responding to a subpoena.

Because of client confidentiality and other rules and regulations, a CPA in receipt of a subpoena should consider the information in the client file and recent communications with the client, or any parties involved, and contact a professional liability risk adviser or attorney before responding.

Read More: How to Respond to Subpoenas

29

Be prepared for kryptonite.

Develop and implement a firm succession or continuation plan in the event of a long-term disability, emergency, or retirement. A continuation plan may help avoid risk exposures such as future lawsuits against the CPA, or his or her estate, and will help spouses, families and heirs figure out what to do.

Read More: Practice Continuation for Small Firms

30

Do I have a conflict of interest?

While conflict of interest issues often arise because of "break-ups" between spouses in a family law matter, many other types of splits can entail a divorce or dispute among shareholders, LLC members, partners and beneficiaries. Some situations may require professional guidance and advice.

Read More: Conflict of Interest

31

Set appropriate policy limits for your firm profile.

Excessively high limits can make your firm a target, however, you need to carry enough limits to protect against a severe claim. A specialized underwriter or agent experienced in CPA firms will work with you to address specific risk areas and appropriate limits.

Read More: What's the Right Policy Limit for Your Firm

32

Don’t lose your Prior Acts coverage.

A firm that is changing from one insurance carrier to another must make the change seamlessly to avoid losing the Retroactive Date (or Prior Acts Date). If the policy is not renewed continuously, the initial Retroactive Date is lost, and a new policy will most likely have a new Retroactive Date. This causes the firm to lose the coverage that it had with an older Retroactive Date, and past professional services that were previously covered would no longer be covered. Always maintain “seamless” coverage, with no lapses in the policy along the way.

Read More: Why It’s Important to Maintain Prior Acts Coverage

EMPLOYMENT PRACTICES

33

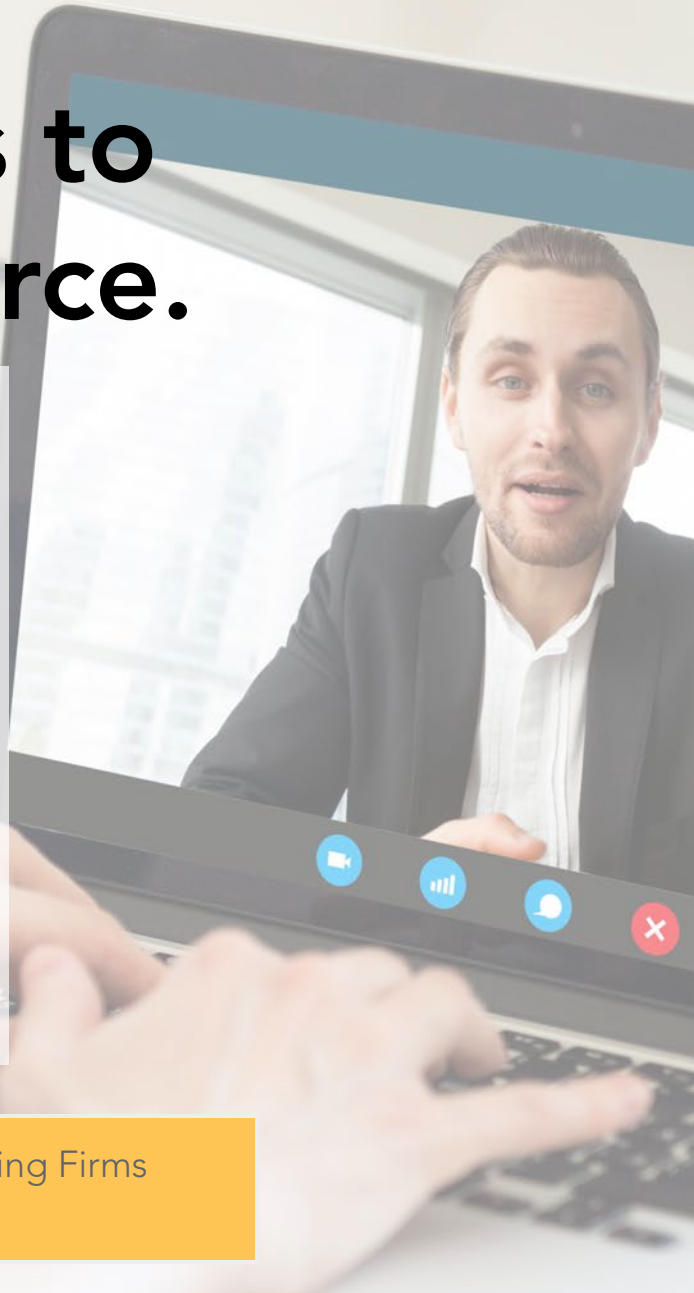
A social media policy is a "must have."

Be sure the firm has a policy that includes a code of conduct, sets forth acceptable and unacceptable communications, and requires certain disclosures and disclaimers, including social media. Have a human resources professional review employee policies to consider whether they inhibit employees' rights.

Read More: Human Resources Policies and Forms: The Backbone of the Firm

34

Implement best practices to support a remote workforce.



These days, as firms consider the various factors needed to support a remote workforce, there are important measures worth taking to minimize increased risks associated with employees working from home. These actions include: **1)** conducting background checks on candidates who are offered a position, **2)** contacting the candidate's references and asking about work habits, strengths and weaknesses, **3)** reviewing and updating policies that impact a remote work group such as cyber safety, use of firm resources, and care of client files and **4)** creating a checklist for an employee's home office to ensure cyber safety.

Read More: Sourcing a Strong Candidate Pool Is Pushing Firms Outside Their Comfort Zone

35

Know what speech is protected in the workplace.

An employer has the right to request that employees remain civil toward each other and refrain from discussion that is not appropriate in the workplace. Employees are free to discuss wages, working hours and conditions with co-workers as protected activity under the National Labor Relations Act. Employees should be able to participate in such conversations without the fear of retaliation, provided they are engaging in "concerted activities" for their "mutual aid or protection."

Read More: What Speech is Protected in the Workplace

Bonus Tip: Looking for CPA-focused insurance and risk management solutions? Give CAMICO a call!

Just as your firm provides the best service, advice and solutions for your clients and community, so does CAMICO by providing CPA-focused risk management advice and guidance from in-house loss prevention specialists and experts. Protecting CPAs for over three decades means that we put our policyholder firms first by embracing a proactive methodology when it comes to loss prevention and claims handling. Simply put, with CAMICO you get high-level technical support with your professional liability insurance and risk management program. Visit www.camico.com for more information or call 800.652.1772 to speak with a CAMICO representative.

CAMICO®

www.camico.com | 800.652.1772