TRACE FORENSIC EXPERTS

Volume 3 | December 2022

Top of Mind

It's hard to believe that 2022 is drawing to a close, and most of us are preparing for a well-deserved rest with family and friends.

As we reflect on 2022, this has been an incredible year for Trace Forensic Experts as we have managed to reach many of our goals and objectives. Trace Forensic Experts has become a major player in the forensic accounting space. This is precisely what our brand is about – it reflects how much we have transformed over the past year, without ever compromising our values, and how we are poised to further grow while creating value for the benefit of all our clients.

The festive season is a magical time to spend with family and friends, splurge on gifts and plan holidays. But it's also an opportune time for fraudsters and scammers. Fraud peaks significantly during the festive season. Fraudsters know that people, frantically shopping and hunting for bargains, are more prone to be off guard at this time of the year.

In 2021, consumers reported losing more than $5 billion to fraud, an increase of more than 70 percent over the previous year, according to data released by the Federal Trade Commission. The most common reported category was imposter scams ($2.3 billion of losses, compared to $1.2 billion in 2020) followed by online shopping scams ($392 million losses, compared to $246 million in 2020).

Below we share some tips so that you can protect yourself from fraud over the holiday period.

1. **Phishing for banking information:** Consumers should be wary when it comes to phishing emails asking them to click on a link to log in to their internet banking profiles to update their details. Banks will never ask their customers to share their one-time passwords or their digital banking credentials (these being the digital banking username and password) by way of a phone call or email. The best way to prevent these phishing scams is to never give out any personal, credit card or other banking information unless you personally initiated the contact.

2. **Never provide sensitive information in an email:** Email phishing forms a large part of identity theft and fraud. You should bear in mind that no reputable company will ever ask for your credit card, bank account or PIN details via email. It's a dead giveaway for a scam or fraud, even if the email may seem legitimate.

3. **Be careful of what you download:** Hackers can gain access to information stored on your computer if you accidentally download malware or spyware. Avoid downloading attachments to emails unless they come from a trusted source. Also, be wary of installing any programs that you may have downloaded. It is advisable to use antivirus software that catches malware or spyware before your computer is infected.

4. **Public Wi-Fi networks:** Unsecured public Wi-Fi networks pose danger if you enter sensitive information while using them. Although hotel and airport Wi-Fi can be convenient, you need to exercise caution and protect against losing credit card information and any other sensitive information. You should also be aware that if a 'free public Wi-Fi' shows up on your device it could be a hacker on a nearby smartphone or laptop attempting to get users to sign on so they can steal your private information. If you really need to use a public Wi-Fi service, then always use a virtual private network (VPN) to protect yourself. Otherwise, you should use trusted authenticated access points or your wireless cellular data connection.

5. **Use strong passwords and use two or more authentication factors:** Always use strong passwords that contain a mix of letters, numbers, and symbols. Multi-factor authentication can provide an additional layer of security for your protection.

6. **Don't save credit card information on websites:** As tempting and convenient as it may be, don't save your credit card information on Google or at e-commerce sites that you frequent. It provides hackers with an opportunity to access your personal information in the event of a data breach.

7. **Use legitimate sites for online shopping:** When shopping online you need to make sure that your details are safe. Always check that there is an 'https' in the web address and an icon of a locked padlock on the left side of the URL. We also suggest that you ensure that the name of the URL is the same as the organization you are transacting with.

8. **Regularly check your banking transaction alerts:** Always check your SMS and email alerts wherever possible. This way, you can flag any suspicious activity straight away.

9. **Protect all personal and sensitive documents.** Lock away your passports and other sensitive documents. Put them in a safe or a place where only a few trusted people have access to. It's not so easy to replace these documents and it's an onerous and costly task fixing the results of ID theft.

10. **Make copies of all your personal and important documents:** If you're going to be traveling this festive season, consider making copies of all your important documents – passports, drivers' licenses, credit cards, etc. It makes the process much easier if you have lost a card or document, or if you have to block a bank account.

Trace Forensic Experts extends a big thank you to all our clients, friends, and business associates. May you all have a wonderful holiday season and a happy and healthy 2023.

Best wishes,

Paul Rodrigues and Deborah Temkin,
Managing Members of Trace Forensic Experts LLC.