https://www.law.com/ctlawtribune/2022/04/21/if-it-seems-too-good-to-be-true-it-may-be-an-attempt-at-identity-theft/

Connecticut Law Tribune

BEST PRACTICES

If It Seems Too Good to Be True, It May Be an Attempt at Identity Theft

Identity fraud reports to the Federal Trade Commission increased nearly 250% from 2016 to 2021, from 400,000 to 1.3 million.

April 21, 2022

By Christine M. Tenore

No matter what area of the law you practice, clients often ask us what to do regarding fear of identity theft. As a "good practices" approach we should have a general idea of how to help protect them.

Since the beginning of the pandemic, many of our clients spent inordinate amounts of time working, record keeping and shopping from home. Our time online has exceeded even the highest projections and the resulting opportunistic scams have mushroomed—not unexpected and as old as Dickensian England (Fagin would be proud)!

Clients should be warned that if something seems too good to be true, take a second look before acting. They are encouraged to act "immediately" because of an offer that is expiring, is an astounding bargain, or in the form of a threat from a pseudo government source. But there is a strong probability that these tactics are an attempt to steal their identity, and their money.

The statistics are alarming. There was a nearly 250% increase in identity fraud reported to the Federal Trade Commission from 2016 to 2021, from 400,000 reported cases in 2016 to 1.3 million in 2020. Where does Connecticut stand? The FTC's Sentinel Network Data Book found that Connecticut has the 12th highest rate of identity theft in the country.

Each state has its own identity theft laws. The laws currently in effect in Connecticut include: Criminal: CGS Sec-53a-129a (2001) and Civil: CGS Sec- 52-571h (2001). Identity theft is classified as an automatic Class D Felony and any prosecuting authority can bring an action. As reflected in the statutes, civil actions are allowed and remedies of greater than $1,000 or treble

damages, in addition to costs and reasonable attorney fees can be awarded if the plaintiff prevails.

For example, las October, judgment was imposed in U.S. District Court in Hartford, sentencing Jaime Pinto to more than 65 months of imprisonment for fraud and identity theft offenses. Pinto and a co-conspirator arranged for vehicle purchases at dealerships in the name of identity theft victims whose personal information included Social Security numbers and dates of birth combined with fraudulent photo IDs. Violations came under the auspices of the US Postal Service, Homeland Security and the local Vernon Police Department.

How do clients know if they've been victimized? Here are few suggestions to share:

- They see an unfamiliar loan or credit account on their credit report.
- They have an unexpected drop in their credit score.
- They receive an unexpected notice from their health insurance company reflecting that they've reached their benefit limit.
- They don't receive expected U.S. mail.
- They try to file their tax return online only to have the IRS reject it, saying a return connected to their Social Security number has already been filed.

We should warn clients shopping on the Internet to avoid typing the name of a retailer into the browser bar—type the website address to prevent being diverted to a fake website that looks real. Vet "new-to-you" businesses by looking for online reviews and searching the Better Business Bureau website for complaints. Check the "contact us" page on a website for a US address and phone number and then call the business to verify. Pay with a credit card—not a bank debit card.

With internet scams, con artists often "phish" for personal data through email, seemingly legitimate requests, claiming information is needed by the victim's bank, credit card or mortgage company. Warn your clients "not to click on unknown links". The criminals ask the victim to verify their financial information by clicking a link, which then could either hijack the victim's information or infect the victim's computer. In addition, victims of online scams often say they did not receive goods purchased which they thought were an online "deal" or a "bait and switch" scheme with high international shipping charges.

Many of our clients go to the library, public cafés or restaurants with free Wi-Fi or other public locations to handle internet research and shopping. You might suggest to your clients that they refrain from browsing on public Wi-Fi because information can be shared unknowingly. At the least, clients should use a Virtual Private Network (VPN) which creates an encrypted connection between the client's computer and the server.

Deed fraud is another area of concern and one we are more likely to be aware of. It occurs when someone steals your client's identity, forges their name on a deed and takes title to a house. When handling real estate transactions, we need to be even more vigilant—checking the title searches, obtaining title insurance and encouraging clients to file for probate when appropriate for protection. Deed fraud usually occurs in the case of a deceased owner and often involves vacation and abandoned homes.

We should encourage clients to limit personal information in a loved one's obituary to minimize notice to potential fraudsters. Sometimes it can be a tenant that perpetrates the fraud, pretending to be the owner.

Tax scams are also prevalent. We should consistently warn our clients not to respond to a call or email requesting personal information from a "tax authority." Electronic tax reminders and "taxpayer advocate" offers are other red flags. Warn your clients that the IRS never calls or emails.

What can clients do if they suspect that they've been the victim of identity theft? Start by placing a fraud alert with one of the credit bureaus:

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

There is a new IRS identity protection tool, as well: an Identity Protection Personal Identification Number that can be found at www.IRS.gov.

As attorneys we are well served to protect clients by attending to their broader needs. Full representation now means giving guidance to protect from possible identity threat issues while providing for current legal needs.

Attorney Christine M. Tenore is a partner at the Fairfield-based law firm, Eliovson & Tenore. She can be reached at http://www.connecticutelderlaw.com/ or 203-336-2566.