Scams Against Lawyers, Professionals, and Other Ordinary People

By Judge Herbert B. Dixon Jr. (Ret.)

Author's Note: As the technology columnist for The Judges' Journal, *I am keenly aware that many scams occur on the lower spectrum of the technology scale, primarily by email and telephone (but sometimes via a non-tech process such as U.S. Postal Service mail). So please grant me your indulgence with this review of some low-tech scams that disrupt the lives of lawyers, professionals, and other ordinary people. Based on my survey of these materials, everyone is a potential scam target regardless of station in life.*

Introduction

Suppose someone asks you to imagine the typical scam victim. You might envision a grandfatherly or grandmotherly figure who is unable to open a new browser tab despite the grandchildren's many efforts to demonstrate the process. While it is true that older adults individually suffer higher losses per scamming incident, most victims of scams are not unsophisticated technophobes. For example, Mary Berners-Lee, a computer programmer, helped create the world's first commercially sold computer. Her son, Timothy John Berners-Lee, is credited with inventing the world wide web!

Notwithstanding this family's technology pedigree, Ms. Berners-Lee was the victim of a courier fraud telephone scam. Scammers convinced her to withdraw money from her bank account and give the money to a special courier, supposedly to help catch dishonest bank employees.[1] Anyone can be a scam victim. Indeed, everyone should be wary of possible scams even in the best of times, but extra caution is warranted in the increasingly digital world necessitated by the pandemic. Amid the COVID-19 pandemic, attempts at fraud have been on the rise. Pre-pandemic, from March 2019 to March 2020, Americans lost $10.5 billion to phone scams; from March 2020 to March 2021, during the first year of the pandemic, Americans lost $29.8 billion to phone scams—nearly three times as much as in the year preceding the pandemic.[2]

Scammers Do Not Discriminate by Age

Scammers target the young and the old. In 2021, the U.S. Federal Trade Commission received over 5.7 million reports of fraud, identity theft, and other consumer protection issues, accounting for $5.9 billion in fraud losses.[3] Of people ages 20–29 reporting fraud to the FTC, 41 percent lost money to the schemes perpetrated, compared to only 18 percent of those in the 70–79 age range reporting fraud.[4] The most common types of fraud and their median losses vary by age group. The top categories for fraud losses for the 20–29-year-old category are $2,000 for fake check scams, $1,821 for job scams, and $1,000 for government imposter scams.[5] For the 80 and over age group, the highest median losses are $7,650 for romance scams; $6,000 for prizes, sweepstakes, and lottery scams; and $4,975 for family and friend imposter scams.[6]

Scammers Understand Their Potential Targets

There is little doubt that scammers target the unsuspecting, but be advised that scammers also target professionals, businesspeople, and other "sophisticated" groups. Scammers are equal opportunity predators.

Judge Herbert B. Dixon Jr. retired from the Superior Court of the District of Columbia after 30 years of service. He is chair of the *ABA Journal* Board of Editors, a former chair of both the National Conference of State Trial Judges and the ABA Standing Committee on the American Judicial System, and a former member of the Techshow Planning Board. You can reach him at Jhbdixon@gmail.com. Follow Judge Dixon on Twitter @Jhbdixon.

According to a psychology professor who has studied scams, scammers are amateur psychologists.[7] They understand that people respond to social influences and authority figures. They know that people do not use all their cognitive resources when stressed. Scammers know that if they can rush people and scare people, the targets become hyperfocused on trying to solve their problem. The high-stress situation induces compliance. Everyone, including persons with law school–honed analytical reasoning skills, entrepreneurs with proven business acumen, and other ordinary people may fall by the wayside if a scammer successfully exploits their vulnerabilities, be it the need to secure payment for services rendered, avoid reputational embarrassment, comply with the law, or satisfy an overwhelming desire to get rich quick.

Scams Against Lawyers

Scams against lawyers take on a variety of schemes, a few of which I will describe below. In addition, scammers also target nonlawyers by modifying these deceitful schemes as needed to fleece the new targets. However, against lawyers, scams often involve purported clients contacting the lawyer with a fabricated legal issue. The fake clients often say they obtained the attorney's name from a reputable attorney in their locality, on LinkedIn, or from a bar referral service or other professional listing. The fake client may request representation as an individual or a company. The issues for which these fake clients request representation are varied, such as loan collection, failure to pay for goods or services, promised compensation for wrongful employment termination, a dog bite claim—you name it. These fake clients often reach out by email and present themselves as out-of-state or from a foreign country.[8]

Some scammers will have constructed detailed aliases with fake, authentic-looking business websites and spoofed email addresses that make an email appear to be coming from the adverse party or a known and trustworthy source. The fake client often sends corroborating documents regarding the dispute and is generally prepared to sign a retainer agreement. After that, the scam can take several paths. For example, the newly retained lawyer may send a notice of representation with a demand to the opposing counsel (the fake information having been provided by the fake client), after which a settlement is reached. Or, after the retainer is signed, the client advises the attorney that the matter suddenly settled and that the purported adverse party (sometimes falsely identified as an existing company) will be sending a check to be deposited in the attorney's trust account for the client's benefit. After the attorney receives the settlement check and deposits it, the client suddenly develops an emergency with an urgent need for the funds and provides wire information to the lawyer.

The scam succeeds if the lawyer wires funds to the fake client before discovering that the check is counterfeit. It is often not understood that it can take weeks for a check to clear, either because checks are frequently processed through intermediaries or because the scammer has tampered with the check (adding or deleting numbers at the bottom of the check to slow down its processing). Almost universally, the depositor of the check will be liable for repayment to the bank of proceeds lost through a bounced check, including any overdraft resulting from a bounced check. Meanwhile, the fake client has absconded with the money forwarded by the lawyer. If the attorney's trust account held funds from multiple clients, as opposed to solely the lawyer's money, then any funds that were transferred from the trust account to the fake client most likely belonged to the real clients, which would trigger an ethical obligation to immediately notify all affected clients,[9] and possibly self-report the event to the bar's ethics or disciplinary office.

A Different Type of Scam

Another type of scam that has proven successful, especially against professionals, occurs when the perpetrator pretends to be someone else to get something from the target. To support their false personae, scammers manipulate caller ID by changing their names and phone numbers to whatever they want. This technique was used against multiple therapists in the San Francisco area who were convinced by a scammer posing as a deputy sheriff that an order to arrest was issued for contempt of court because the therapist had failed to make a court appearance to give testimony despite having received and signed for a subpoena.[10] In one case involving this scheme, the therapist told the scammer that she had never received a subpoena. In response, he said to her that she would have to come to the sheriff's office to prove that her signature had been forged and that to avoid being held in jail upon her arrival, she could pay in advance a $6,000 bond that would be reimbursed once she proved the forgery.

Over several hours, the fake deputy sheriff convinced the therapist to buy prepaid Visa gift cards and share the card numbers and PINs (located under the scratch-off area). During this time, the scammer alternated between being friendly and scaring the therapist with the prospect of being held in jail and losing her license. When the therapist came across a flyer about common scams while purchasing the gift cards at a drug store, she confronted the fake deputy sheriff about whether he was perpetrating a fraud. He responded by telling her he could prove he was legitimate by calling her from his desk phone at the sheriff's office. The scammer instructed the therapist to Google the sheriff's office number where he supposedly worked. When he called her back, the sheriff's office number indeed appeared on the therapist's caller ID. Following this challenge and response, the scammer made his victim feel guilty, asking how this could possibly be a scam with him calling her from the sheriff's office. This diabolical scheme was successfully implemented against several therapists in the San Francisco area.

Once the therapist provided the fake deputy sheriff with the Visa card numbers and the PINs, the final step of the scam involved his advising the therapist that she should put the cards in an envelope with his name and badge number and deposit the envelope in a special mailbox (which was a regular, public mailbox) and that a prearranged pickup with special courier delivery to the sheriff's office would occur. In reality, the card and PINs provided the scammer with everything needed to access the money. However, having the victim deposit the cards in a mailbox would delay or thwart any law enforcement

investigator's ability to access specific identification information about the cards.

Tech Support Scams

Another category of scams is the tech support scam, usually starting with an unsolicited phone call from scammers impersonating tech support staff or a pop-up window on the target's computer screen. The scammer often claims to work for an established tech company and informs their target that a threat to the consumer's computer has been detected. Next, the scammer requests remote access to the computer to run diagnostic tests to help get rid of the fictitious threat. The scammer then convinces the victim to pay for repairs, software, etc., to combat the nonexistent problem. During this process, the scammer acquires the victim's credit card information and may put actual malware on the victim's computer to steal more personal and financial information. When this scam occurs through a pop-up window, the scammer may be a person or an automated computer program controlled by artificial intelligence.

A Profitable Scam Through the U.S. Mail

Finally, readers should be aware of scams involving no technology, for example, a scam through the U.S. mail. In Washington State, a single scamming operation used the state's online public records and registration requirements to scam more than 15,000 entrepreneurs out of $1.2 million.[11] Using similar schemes, two scamming operations in the state cleared $3.6 million nationally. The scammers used envelopes with a localized address that gave the appearance of government paperwork and included an invoice for $82.50 for a "Certificate of Status" or workplace poster to stay registered in their state. One of these companies called itself "WA Certificate Services" and included a state address to appear legitimate. A variation on this scheme by others has taken a similar approach by charging amounts under $100 for a workplace labor poster that the scammers said was mandatory. Following this same approach, a scammer in Virginia posed as "Virginia Certificate Service" and used a UPS store service that forwarded payments to the scammer. This type of scam is usually most successful against sole proprietors and small business owners wearing multiple hats as manager, accountant, human resources, and marketing—with no separate legal team.

Final Thoughts: Exercise Caution

As I warned at the beginning of this column, neither age, tech-savviness, nor professional accomplishment defines the typical scam target. Anyone can be a victim. While there is no surefire way to avoid being a victim, there are good habits to develop to reduce the probability of succumbing to one of these schemes.

Watch for messages replete with grammatical errors. Be cautious of notices that you have won a prize or a deal that seems too good to be true. Look carefully at email and web addresses to ensure they are legitimate. Verify an official-looking email address or domain name before disbursing funds. Lawyers and other professionals should consider setting up a Google alert for their businesses, which may catch fake entities appropriating their identities. To avoid being caught in legal representation scams, lawyers should never disburse funds to clients immediately. Wait until the check has cleared and the funds are actually in your bank account (instead of provisionally credited subject to collection). Consider contacting the issuing bank about the validity of the check. Look up the bank's contact information independently rather than relying on the information on the check or from the new client.[12] Be extra wary of a check from an unknown party or related to a new client; ask questions and take the time to confirm that the party is who they claim to be. Finally, while not a foolproof method of deterring scammers, consider holding videoconferences with new clients. That process may deter some con artists because scammers usually prefer to communicate exclusively over email and will be reticent to join a videoconference.

If you suspect you might be the target of an email, telephone, or other scam, report the incident to an appropriate authority, such as the Internet Crime Complaint Center on the ic3.gov website, local police, the Federal Bureau of Investigations, and even the nearest Secret Service field office. Victims of scams tend to be reluctant to seek help or come forward to share their stories due to embarrassment. However, spreading awareness of the different kinds of scams that one might encounter is one of the best ways to prevent others from falling victim to them. ■

Judge Dixon wishes to thank Amanda Purcell, Esquire, Superior Court of D.C. senior judges' law clerk, for research and writing assistance preparing this article.

Endnotes

1. *Mary Berners-Lee: An Unlikely Fraud Victim*, BBC (June 4, 2014), https://bbc.in/39OVx0I.

2. Carolyn Said, *"He Held Me Hostage with No Gun but with His Words": The Phone Scam Gaslighting Therapists*, S.F. Chron. (Sept. 27, 2021), https://bit.ly/3ErRXop.

3. Fed. Trade Comm'n, 2021 Consumer Sentinel Network Data Book 2, 5 (Feb. 2022), https://bit.ly/3rCmdrE.

4. *Id.* at 4.

5. Fed. Trade Comm'n, Consumer Sentinel Network: Age and Fraud Infographic (Mar. 31, 2022), https://tabsoft.co/3z8vkF1.

6. *Id.*

7. Said, *supra* note 2.

8. Examples of these inquiries can be found on a blog titled "Attorney Email Scams" located at https://lawyerscam.blogspot.com.

9. *See* Model Rules of Pro. Conduct r. 1.4(a)(3) (Am. Bar Ass'n 2020) (lawyer shall "keep the client reasonably informed about the status of the matter"); ABA CPR Pol'y Implementation Comm., Variations of the ABA Model Rules of Professional Conduct, Rule 1.4: Communications (Aug. 21, 2021), https://bit.ly/3Gw1SKS.

10. *See* Said, *supra* note 2.

11. Sean Salai, *Fake Government Fee Scam Nets Millions from Small Businesses*, Wash. Times (Mar. 18, 2022), https://bit.ly/3lX6PCV.

12. A convenient tool for finding contact information for banks insured by the Federal Deposit Insurance Corporation is located at https://bit.ly/3x3zRGh; the equivalent for federally insured credit unions is located at https://mapping.ncua.gov. Another resource is the Office of the Comptroller of the Currency's website, which issues alerts for counterfeit checks at https://bit.ly/3PWKO4P.