Susan Whittaker
Testimony before the United States Senate Special Committee on Aging
"Fighting Fraud: How Scammers are Stealing from Older Adults"
September 19, 2024

Chairman Casey, Ranking Member Braun, and Members of the Senate Special Committee on Aging, thank you for inviting me here today to share my story. My name is Susan Whittaker. I am an Administrative Assistant for the Executive Director of Lehigh County Aging and Adult Services in Allentown, PA. I have been in my current position for four years. My previous employment was for 45 years at The Morning Call, our local newspaper, and a subsidiary of Tribune Publishing.

I am presenting testimony today because my late husband, Bill, was the victim of a scam. I will also share the steps I took once I knew the scam had happened, and the unavailability of the bank we entrusted with our personal account and the business account.

It was a Tuesday night and when I got home, Bill was more quiet than normal. I thought he was just having an off day. He didn't talk a lot the next few days. Bill suffered from dementia and Alzheimer's, diabetes, congestive heart failure, pulmonary embolisms, neuropathy, and gout. At the time of the scam he was 75. Although Bill had sold his business, Bill Whittaker & Son Construction LLC, to his son, Bill stayed on as the office manager. He took care of ordering materials, making payments, and submitting payroll—all the office responsibilities. As the week went on, Bill seemed to be quieter and not talking about anything; he seemed worried.

On Friday night when I came home from work, he started to tell me what had happened. He told me he received an email from QuickBooks, which was used to manage bookkeeping for the business. The email said that the business account had been charged $499 for an upgrade. He said he didn't order the upgrade. He contacted what he thought was QuickBooks at that point. This person told Bill that in order for him to refund Bill's money, Bill needed to first pay him $500 and then "QuickBooks," who was really the scammer, would send it right back to him via another payment platform. He was told not to share this with anyone because then he would not be able to get his money back.

Bill was instructed to install an application on the computer so he could transfer the funds directly into the scammer's checking account. He walked Bill through step by step on what he needed to do to give the scammer online access to install the software. Bill also scanned and sent him a copy of his Social Security card and driver's license. Once everything had been setup, the scammer had Bill set up a Venmo account. Finally, he showed Bill how to transfer the $500 via Venmo. Because the scammer had access to the computer, as Bill was in the middle of typing the number 500, the scammer took control through the software and added an extra zero to the $500. Now the transfer was for $5000. He started yelling at Bill for making the error, when in reality Bill had not made a mistake. He then told Bill, "Look what you've done." He said that now Bill needed to send him $5000 in order for him to send back the $5000.

That Friday night when I spoke with Bill, he shared with me that now, in addition to the $499 initial fraudulent upgrade fee that needed to be refunded to the business account, this individual now owed us money from our personal accounts, due to the numerous Venmo transfers. Bill said that this individual would be calling him back that night at 6pm. The phone rang promptly at 6pm.

This time, I answered the phone.

The scammer on the other end of the phone was totally surprised to hear someone other than Bill. I asked him to explain the situation we were in. He walked me through all of the charges and Venmo transactions and I questioned his logic and the process he had put Bill through. At this point, I knew it was a scam, but I asked him to please check with his boss. He said he would call me back, and I told him I would be waiting for his call. At this point, I wasn't even sure how much money had been taken from our personal account and the business account.

While waiting for a call back, I shut down the MAC and booted it back up. I created a new login account and deleted the old information. I found the software, which had been installed, and uninstalled it and changed the settings the scammer had set. I also contacted our bank, Truist, through their customer service department. I wanted to put a hold on both accounts to stop the money from being transferred. Since it was after 6pm, customer service was closed until Monday morning at 8am. Then I called their fraud phone number. They, too, were closed until Monday morning at 8am. Fortunately, we knew the bank manager at the local branch. Bill called him and asked for his help. He said he would do what he could, but wasn't sure he would be able to get any money back or stop any transfers. There never was a call back from the scammer.

Monday morning, while I was at work, Bill called local law enforcement. They spoke with him, and said they would be in touch with the bank and would work with them. The person Bill spoke with was very kind and patient. During that time, I put a stop on all credit reporting, a hold on all accounts and called the Truist headquarters in North Carolina. I never did get to talk to anyone there.

In the end, the scammer took a total of $28,000 from us. However, the bank, along with law enforcement, recovered $8,000 of the money taken from our accounts. Because I acted so quickly, they were able to stop these funds before they were dispersed. Despite this, we still lost a total of $20,000—$10,000 from our personal accounts and another $10,000 from the business account.

This scam was devastating and had a devasting effect on Bill—both financially and emotionally. Because we lost $20,000, and Bill had a lot of chronic health conditions, Bill began to ration his medications. We just couldn't afford them anymore. Bill also felt responsible and felt he owed it to his son to repay the money. He kept saying he was sorry and that he was so stupid. He asked how could he make such a stupid mistake. I assured him that he was only trying to save the business $499, and that he didn't do anything wrong. For several days, he was very quiet. After the scam, Bill would not answer the phone unless he knew the phone number and he would not open his email until I reviewed it. In addition to not answering emails or phone calls, Bill started to doubt himself in everything he needed to do. His son no longer allowed him to do any office work and so Bill lost his job. He also lost his sense of self-worth. I was really sad to see this very intelligent and past business owner, become so afraid to read emails and use a phone. It was a huge setback for him, and I think contributed to his worsening health conditions. One thing that I learned is that any event such as this has a devasting effect on the victim regardless of the situation and the scam.

Thank you.