Good day. My name is Glenn Daigon. For over 25 years, almost my entire professional career, I have worked as a researcher in the labor movement. Much of my work consisted of due diligence background checks against nonunion companies, business executives, and candidates running for office. Yet my experience in finding lawsuits, regulatory violations, and criminal records on all of the groups mentioned, did not prevent me from falling victim to a scam.

In May of 2024 my online bank account was hacked, and I had to shut it down and transfer funds to a new account. Six weeks later, while online at my home personal computer, I lost total control, my keyboard did not work, and a message filled the screen that Microsoft was initializing and not to turn off the computer. It was an obvious hack, the second one in six weeks.

I tried to go on the Microsoft site and contact help but kept getting timed out. So, I Googled the Microsoft help phone number and contacted them. The phone number was listed on a site which looked legitimate and had all the Microsoft logos. It turns out it wasn't---it was a well-disguised scam number.

They informed me that they could only handle technical issues and for security matters they would refer me to their security contractor. I was put in touch with someone who identified himself as Officer Mike Wilson, with the National Crime Agency, (NCA), headquarters in London. He referred me to their website and told me his team cooperated with ATF, Border Patrol and other law enforcement agencies against international hackers.

In hindsight, before allowing him on my computer remotely, I should have done proper due diligence and at the very least, contacted the NCA in London to see if he was legitimate. Spoiler alert---he was not. But I have consistently heard stories of hacked bank accounts getting cleaned out in under an hour and that issue seemed to be the most immediate one to take care of.

Unfortunately, I let "Officer" Wilson access to my computer to stop the hack. He won my trust in the following ways:

- He went online and showed me my bank checking account records and how in the last 24 hours there had been several attempts to withdraw funds, underlining the urgency of action.

- He showed me a downloaded malware file titled Zeus on my PC, then copied and pasted the entire file name in GOOGLE. The GOOGLE hits that came up showed this malware was specifically designed to hack into and drain financial accounts.

- He also told me that hackers had used my personal information to set up phony financial accounts and passport accounts in my name. This echoed almost word for word what my bankers told me would happen when hackers got a hold of personal information.

- Wilson had a record of my phone calls, including the one to the scam Microsoft number. That helped firm up my belief that he was a legitimate law enforcement officer. Who else would have access to this kind of information?

- During our phone conversations when we were online, I lost control of my computer, and someone remotely started moving the cursor. Wilson immediately told me to shut off the computer. Later, Wilson showed me evidence that efforts were being made to hack my annuity accounts (through emails showing that people had tried to login to those accounts). He convinced me that shutting down the annuity accounts and transferring the money to my checking account would enhance security.

- At this point I was angry at being hacked twice in the space of six weeks. I felt if the hackers were not caught, this pattern might keep repeating itself unless I pulled the problem up by the roots. Wilson said his agency could catch the hackers via the NCA depositing money into my account, and then my withdrawing it and placing them in bitcoin accounts. He said when the criminals went to withdraw the bitcoin account money, they would give away their locations and be arrested.

- He would show me multiple times online the “government money” being deposited into my account and then have me withdraw that amount and put it in bitcoin accounts. After about ten days he sent me detailed profiles of two of the supposed crooks that the NCA had picked up after they withdrew the money. The profiles contained highly detailed personal information and a criminal history for both. In my opinion, they looked like they could only have come from a law enforcement database and that progress was being made towards bringing the hackers to justice.

- When at one point I got suspicious of what was going on and reported it to the police, Wilson forwarded me a memo supposedly from the FTC referencing that my personnel information was on financial and passport accounts. The memo looked like it was very professionally written.

In summary, for all of the above reasons, Wilson looked like a legitimate law enforcement officer who had my interests at heart. He would mention frequently in phone conversations that the tax liabilities incurred by my withdrawing money from the annuity accounts would be paid for by the NCA.

He also mentioned that at the end of his team’s investigation, their staff would contact the security departments of the banks involved and let them know what was going on.

The reality of course was different. There was no “government money” being deposited into my account. I was unknowingly withdrawing my own funds and by placing them into bitcoin accounts, throwing that money away. And it is highly likely that the threats to my account were caused by Wilson himself, not remote hackers. I wound up losing about a third of my retirement funds.

“Officer” Wilson was not your garden variety scammer. He probably had a law enforcement background and access to a lot of resources to bamboozle his victims. If someone with my experience can be taken in, I think he and his kind represent a very dangerous threat to the average person.

All of the money from the dissolved annuity accounts was stolen. Unfortunately, to add insult to injury, I have to pay hefty federal and state taxes on this stolen money.

Given how sophisticated online scammers are it is very easy for anyone to fall victim to them. In my case, I made the mistake of calling a well-disguised scam help number that set things in motion. To place a tax on stolen funds is grossly unfair and only makes a bad situation worse for those victims.

For that reason, I urge you to support Delegate Vogel's bill to change state tax law so that scam victims are not held liable for stolen funds.