HOUSE INDUSTRY, BUSINESS AND LABOR COMMITTEE
JONATHAN WARREY, CHAIRMAN
JANUARY 22, 2025

TESTIMONY BY
ELIN S. ALM
DIRECTOR, CONSUMER PROTECTION AND ANTITRUST DIVISION
OFFICE OF ATTORNEY GENERAL
RE: HOUSE BILL NO. 1447

Mr. Chairman and members of the Industry, Business, and Labor Committee. I am Elin Alm, and I serve as the Director of the Attorney General's Consumer Protection and Antitrust Division. I appear on behalf of the Attorney General in support of House Bill No. 1447 and to provide some background on the significance of House Bill No. 1447 for consumer protection.

Over the last few years, the Attorney General's Office has noticed a substantial increase in reports of scammers employing the use of virtual currency kiosks. Data from the Federal Trade commission shows that fraud losses at virtual currency kiosk have skyrocketed and increased nearly tenfold between 2020 and 2023. Most of the scams employing the virtual currency kiosks are government impersonation, business impersonation, or tech support scams. Numerous North Dakota residents have reported loss of significant amounts of money to scammers instructing them to deposit money into the virtual currency kiosk to safeguard their money or to make supposedly required payments. To illustrate how the virtual currency kiosk is used in scams, I will provide a few real examples of the reports we received in 2024, where the reported losses exceeded half a million dollars:

- On May 2, 2024, an elderly Bismarck woman received a Microsoft pop-up on her computer. She called the number and talked to "Austin" who represented he was with fraud protection and that $30,000 had been taken from her account. The woman was told that her bank and the Federal Reserve were also involved. She was instructed to remove all her money from her bank and deposit the money into a "Federal ATM machine." She made two deposits ($20,000 & $12,000) at the virtual currency kiosk at a gas station. When she was prevented from sending more through that machine, she was instructed to make an additional two deposits ($15,000 & $25,000) at a virtual currency kiosk at a grocery store. The woman later went to her bank and learned she had been victim of a scam and had lost the $72,000 that she deposited in the virtual currency kiosk.

- In August of 2024, a Bismarck woman was experiencing issues with her iMac computer and searched for a phone number for Apple support on the internet. She found a number represented to be for Apple Support. When she called the number, she was told her devices were compromised and there were charges on her accounts. The scammer gave her what he represented to be a claim number with the FTC and proceeded to help the woman reach out to what the scammer called her banks' "headquarters". The person at the banks' "headquarters" told the woman she needed to start a virtual account, take cash out of her bank, and deposit it into a "federal public machine" so the money can be traced federally to know she is attempting to fix the supposed problem. She then proceeded to put $10,000 into a virtual currency kiosk as instructed, thereby transferring the $10,000 to the scammer.
- In September of 2024, a 41-year-old Bismarck woman received a phone call from an individual who identified himself as being with the Burleigh County Sheriff's Office. The scammer claimed that the woman had failed to appear on a federal warrant and was in contempt of court. She was instructed to send $5,500 through a virtual currency kiosk to pay the fine and clear her name. Consequently, she withdrew $5,500 from her bank and deposited the money into a virtual currency kiosk at a grocery store in Bismarck, thereby losing the money to the scammer.
- In October of 2024, a 63-year-old Dickinson woman fell victim to a government imposter scam when she was told that because of Identity Theft, she was going to be arrested for money laundering. She withdrew $13,000 from her bank account and was told to deposit the money in a virtual currency kiosk for "safe keeping," when in fact she was sending it to the scammer. She was then instructed to pull another $70,000 from her retirement account. Luckily, her employer intervened before she lost additional funds.
- In October of 2024, a 62-year-old Carrington man reported that he was a victim of a Pig Butchering scam. The man had entered an online relationship with who he believed was a female. The female subject had recommended that he begin investing in Bitcoin, to which he agreed. During this scam, the man went to multiple virtual currency kiosks and purchased approximately $354,500.00 in Bitcoin, all of which were transferred to the scammer and lost.

So far in January of 2025, three North Dakota residents have already reported losses in the combined amount of $34,000 to scams that involved the use of virtual currency kiosks. Two reports involved Jury Duty Scams with losses of $9,000 and $9,500. The third report involved an Account Compromise Scam where the consumer lost $15,500 transferred to the scammer through a virtual currency kiosk after she was falsely led to believe that an

error had been made resulting in her receiving a $19,999 refund on a fraudulent charge when she was only entitled to a $199 refund.

Virtual currency kiosks are a particularly advantageous tool for scammers because the transactions are immediate and cannot be called back like a wire transaction, cancelled like a gift card, or intercepted like a package. The virtual currency kiosks provide an instant and easy one-step method to steal money from consumers, because it eliminates the opportunity for victims to stop or reverse the transaction when they realize they have been scammed. Scammers are also able to take advantage of consumers unfamiliarity with virtual currency and the purpose and functionality of the virtual currency kiosks.

House Bill No. 1447, if enacted, can help protect every North Dakota resident from losing money to a scam. Scammers are becoming more sophisticated and manipulative, and scams can ensnare even the most intelligent and financially savvy person. Scammers are criminals whose playbook includes the employment of a psychological warfare to steal consumers hard earned money. Many scams start with a call or message about supposed suspicious activity or unauthorized charges on an account or a fake security warning on a computer, and such messages are hard to ignore.

It's important to keep in mind that under the right circumstances, anyone can become a victim of a scam. We know the prevalence of scams is much higher than what's reported. Because there is a stigma that remains around scams - the misconception that victims are naive, unintelligent, uneducated, or experiencing cognitive decline - victims feel helpless, ashamed, alone, and are unwilling to report incidents of fraud. We often hear from scam victims, who are willing to report, that they are ashamed and embarrassed because they feel they should have known better and cannot believe that this happened to them. It may be easy with the benefit of hindsight to see the signs of a scam. However, when you are in a situation where you are contacted by someone with apparent authority, with threats of serious consequences unless you take swift action as instructed to protect yourself, your family, or your money, it does not appear or feel like a scam.

While the existence of scams is a global problem that is hard to combat, there are measures that can be put in place to at least make it harder for scammers to perpetrate and profit from scams against North Dakota residents. House Bill No. 1447 represents such a measure through its required display of warnings and disclosures and the daily limit on transactions. Therefore, the Attorney General supports a "Do Pass" recommendation on House Bill No 1447. Thank you for your time and consideration. I would be happy to try and answer any questions.