DIFI Alerts Arizonans: Stay Vigilant Against Evolving Scams Aimed at Financial Exploitation

PHOENIX, AZ – The Arizona Department of Insurance and Financial Institutions (DIFI) is alerting consumers about the persistent and evolving threat of scams designed to defraud individuals of their hard-earned money. Fraudsters continuously adapt their tactics, often impersonating trusted entities and exploiting new technologies to pressure or trick potential victims.

Recent trends show scammers leveraging various methods, including government impersonation texts, as well as schemes involving virtual currencies like Bitcoin. These methods are merely tools in a scammer's arsenal, all with the ultimate goal of extorting money from unsuspecting Arizonans.

"Scammers are relentless in finding new ways to exploit vulnerabilities, whether it's through a convincing text message or by leveraging unfamiliar financial concepts," said DIFI Chief Deputy Director of Finance, Deian Ousounov. "It is important for Arizonans to be aware of these deceptive practices and to take proactive steps to protect their finances and personal information."

Common scam tactics to watch out for include:

- **Virtual currency kiosks/ATM Scams:** There has been a rise in fraud involving virtual currency kiosks/ ATMs. If someone asks you to pay or deposit money through a virtual currency kiosk/ATM, it has the potential to be a scam, especially if the request is not from a trusted institution. While some businesses deal in virtual currencies, most financial institutions do not accept or request payments via virtual currency kiosks/ATMs. Be extra vigilant when sending or requesting payments in virtual currencies and verify each request through official channels. Protect yourself, never send cryptocurrency to strangers or under pressure.
- **Impersonation Scams:** Fraudsters pretend to be government agencies (like ADOT or USPS), businesses (such as financial institutions or insurance companies), or even law enforcement. They may claim you owe money, your accounts are compromised, or there's a legal issue. They often pressure victims into immediate action, such as disclosing personal information and instructing them to wire funds or withdraw funds from their bank accounts and purchase and transfer cryptocurrency or gift cards.

- **Investment Scams:** Scammers, sometimes posing as financial advisors or even friendly acquaintances on social media, promise high, "zero-risk" returns if you invest in cryptocurrency through them, or other fake schemes.
- **Blackmail Scams:** You may receive emails or physical mail to your home threatening to expose embarrassing personal information unless you pay a ransom, often demanded in cryptocurrency.
- **Emergency Scams:** Scammers prey on your emotions by impersonating a loved one (grandchild, child, etc.) in distress, claiming they need money immediately for an emergency (e.g., bail, medical bills, travel). They often ask for payment via wire transfer, gift cards, or cryptocurrency, and tell you to keep it a secret.
- **Social Engineering Scams:** Fraudsters often employ tactics designed to exploit a person's trust to convince the victim to willingly disclose their confidential information. Fraudsters typically utilize social media, telephone, or in-person tactics to initiate contact with potential victims and try to build a relationship before asking victims to disclose information or transmit funds.

Helpful Hints to Protect Yourself from Scams:

DIFI urges all Arizonans to keep the following in mind when encountering suspicious requests, especially those related to financial or insurance matters:

1. **Legitimate insurance companies and financial institutions will NEVER ask you to provide personal information or to pay with a gift card, cryptocurrency, or through a payment app in unexpected requests.** This is a major red flag that indicates a scam.
2. **Verify Information Independently.** Before taking any action, especially involving financial transactions, always hang up or delete the message. Independently verify the legitimacy of the caller or sender by directly contacting the organization they claim to represent. **Never use the contact details provided in the suspicious request.** Instead, use the phone number listed on your official statements, the company's official website, or the back of your credit or debit card.
3. **Verify the Entity's Status**. Many businesses that operate in Arizona need some sort of registration or license, and bonding requirements to operate in our state. Verify an entity's legitimacy through official registries, like the Arizona Corporate Commission website, or DIFI's licensing search section. Additionally, check if the entity has been

reported for scams or improper acts through websites such as the Better Business Bureau, Google Reviews, and the Federal Trade Commission. Finally, research the entity's website and its overall footprint to determine if its business operations are legitimate.

4. **Do Not Engage or Provide Personal Information Without Verification.** Consumers should never provide their passwords under any circumstances. Never engage with an unexpected requestor or provide sensitive personal information (such as your Social Security number, bank account details, passwords, or driver's license number) unless you have first verified that the person or organization is legitimate using a trusted contact method (e.g., a phone number from your official statement).
5. **Be Skeptical of Pressure Tactics:** Scammers often create a sense of urgency, pressuring you to act quickly before you have time to think or consult with others. Take your time, do your research, and discuss any suspicious requests with a trusted family member, friend, or regulatory agency.
6. **Secure Your Personal Information:** Protect sensitive accounts by using multi-factor authentication. Never click on unexpected links in texts, emails, or social media messages, even if they appear to come from a known company.
7. **Delete Suspicious Communications:** Ignore messages from unknown numbers, and delete all suspicious texts. Look for red flags, such as misspellings or grammatical errors. Even if a message asks you to "text STOP," do not respond, as this can confirm your number is active.

How to File a Complaint:

If you believe you or someone you know has been the victim of a scam or consumer fraud, it is crucial to report it immediately.

- You can file a consumer complaint with the **Arizona Attorney General's Office** by visiting www.azag.gov/consumer. If you need a complaint form sent to you, you can contact their office in Phoenix at (602) 542-5763, in Tucson at (520) 628-6648, or outside the Phoenix and Tucson metro areas at (800) 352-8431.
- You can also file a complaint with the **Federal Trade Commission (FTC)** on their website at reportfraud.ftc.gov or get help with identity theft by visiting www.identitytheft.gov or calling (877) 438-4338.

Awareness and vigilance are your best defense against these fraudulent activities. DIFI remains committed to educating and protecting Arizonans from financial and personal exploitation.