GARY R. HERBERT
Governor

SPENCER J. COX
Lieutenant Governor

State of Utah
Department of Commerce

FRANCINE A. GIANI
Executive Director

DANIEL O'BANNON
Director, Division of Consumer Protection

June 19, 2019

MEDIA ADVISORY

"Utah Consumer Alert: Beware of Fake Wells Fargo Crucial Notice Text"

"Division of Consumer Protection reports phony texts are targeting Utah consumers with fake 'crucial' bank alert, asking them to call Wells Fargo with account information"

(For immediate release…)

SALT LAKE CITY, Utah - Francine A. Giani, Executive Director of the Department of Commerce, announced today that the Utah Division of Consumer Protection has received a report that phony texts pretending to be from Wells Fargo Bank are being sent to consumer phones. The "crucial" account alert text asks the recipient to call a phone number that leads to a recorded message claiming that the person's Wells Fargo bank account was compromised and that bank needs to confirm important personal information. The recorded message then prompts the consumer to enter the following information into their phone pad so that their ATM card can be reissued; Wells Fargo ATM card number, social security number, Wells Fargo ATM card pin number, Wells Fargo ATM card expiration date, Wells Fargo 3-digit security code on back of ATM card, billing zip code, and last known checking account balance. According to Wells Fargo Bank, this texting scam has been reported in neighboring Western states but had not been reported previously in Utah.

"This phony text message came across my cell phone and looked so convincing that if I did have a Wells Fargo account, I might have taken the bait," admitted Francine A. Giani. "Our biggest concern is that young people who use their cell phones for all aspects of their lives could easily fall for the bait. Please share this consumer alert with your friends and family."

A Utah Division of Consumer Protection investigator called the phone number and entered false information into the key pad. Upon conclusion of the entries, the recorded message informed the investigator that their Wells Fargo ATM card had been reissued. This scheme is an example of what is commonly known as an Imposter Scam where someone pretends to represent a real entity such as Wells Fargo Bank to dupe the consumer into revealing personal account and identity information to the fraudster.

What Consumers Need to Know about Imposter Scams

1) Imposters will pose as people, companies or government entities that you are familiar with to set the trap via text, email or phone calls.

2) Imposters will try to create an emergency to make their targets emotionally react to a request, such as confirm personal account or identity information.

3) Imposters will ask for information known entities would not normally ask you to confirm over the phone such as your Social Security Number.

4) Imposters will ask you to pay for fines, bills or fees through nontraditional financial means such as gift cards or wiring money.

What Consumers should do about Imposter Scams

1) Don't ever give out personal information or bank account details to anyone over the phone. This also goes for your Social Security if someone asks you to confirm the last 4 digits of your number.

2) Anyone who tells you to wire money, pay with a gift card, or send cash is a scammer. Always. No matter whom they say they are.

3) If you're worried about a text or call from someone who claims to be from a known business or government agency, hang up the phone and call the established contact numbers published for the real company or government agency to find out more information.

Wells Fargo Consumer Tips for Account Holders

These types of text messages and phone calls are indeed scams. The attempts are becoming more commonplace, and we advise all consumers to:

• Use caution if you receive an email or text expressing an urgent need for you to update your information, activate your online banking account, or verify your identity by clicking on a link.

• If you receive an email or text message requesting sensitive information, do not respond. Delete it.

• If you receive a suspicious phone call requesting your information or access to your account, hang up and contact Wells Fargo directly to verify the call at 1-800-TO-WELLS (1-800-869-3557). The number is on the back of your debit/credit card.

• If you are a Wells Fargo customer who received this text message and clicked on the link or provided information via phone, call us immediately at 1-866-867-5568.

For more information on how to protect yourself from scams or to file a complaint, log on to the Utah Division of Consumer Protection website at: www.consumerprotection.utah.gov

---

For media enquiries contact:
Jennifer Bolton
Public Information Officer
Utah Department of Commerce
(801) 530-6646 office
(801) 652-8322 cell
jenniferbolton@utah.gov
Follow us on Twitter @UtahCommerce