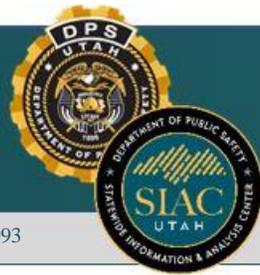


Utah Department of Public Safety
Statewide Information and Analysis Center



Intelligence Note

SIAC@Utah.gov Phone: 801-965-3838 Fax: 801-969-0808

June 11, 2020 SIAC - 093

COVID-19 Fraud: Utah Case Report

Release: 1500 Hours, 6/11/2020

(U) Summary

(U//LES) The Utah Statewide Information and Analysis Center analyzed local, state, and federal data to determine the scope of COVID-19 related fraud cases in the State of Utah. COVID-19 is mentioned over 3000 times in Palantir reports (from January 2019 to June 2020) with an average of 30 mentions per week in May and June 2020. Of that total, roughly 37 cases were identified as COVID crime related. The SIAC also reached out to the Federal Bureau of Investigation, Department of Homeland Security, and other Utah based federal partners to determine the number of Utah COVID related fraud cases being handled by those organizations.

(U) Key Information

(U//LES) Out of the 3000 mentions of COVID-19 in Palantir, only 37 are COVID crime related with 5 listed as fraud crimes.

(U//LES) The Federal Bureau of Investigation and the Federal Trade Commission report seeing a significant increase in COVID-19 fraud reports.

(U) Background Context

(U//LES) According the Federal Bureau of Investigation website, the most common types of COVID fraud are:

- Government Impersonators
- Fraudulent Cures or Medical Equipment
- Work-From-Home Fraud
- Investment Fraud

(U//LES) According to reporting from DHS in April 2020, the COVID-19 pandemic would likely increase hostile cyber actors' ability to target U.S. public health and healthcare sectors. By exploiting the fears caused by the pandemic, individuals are more likely to open documents and click links related to COVID-19 before verifying their legitimacy. According to a public cybersecurity firm's research project, the following cyber-attack methods were used; credential phishing, malicious attachments, malicious links, landing pages, downloaders, spam, and

malware. The Federal Trade Commission reports over 37,000 fraud cases reported to their offices between 1 January, 2020 to 9 June, 2020.

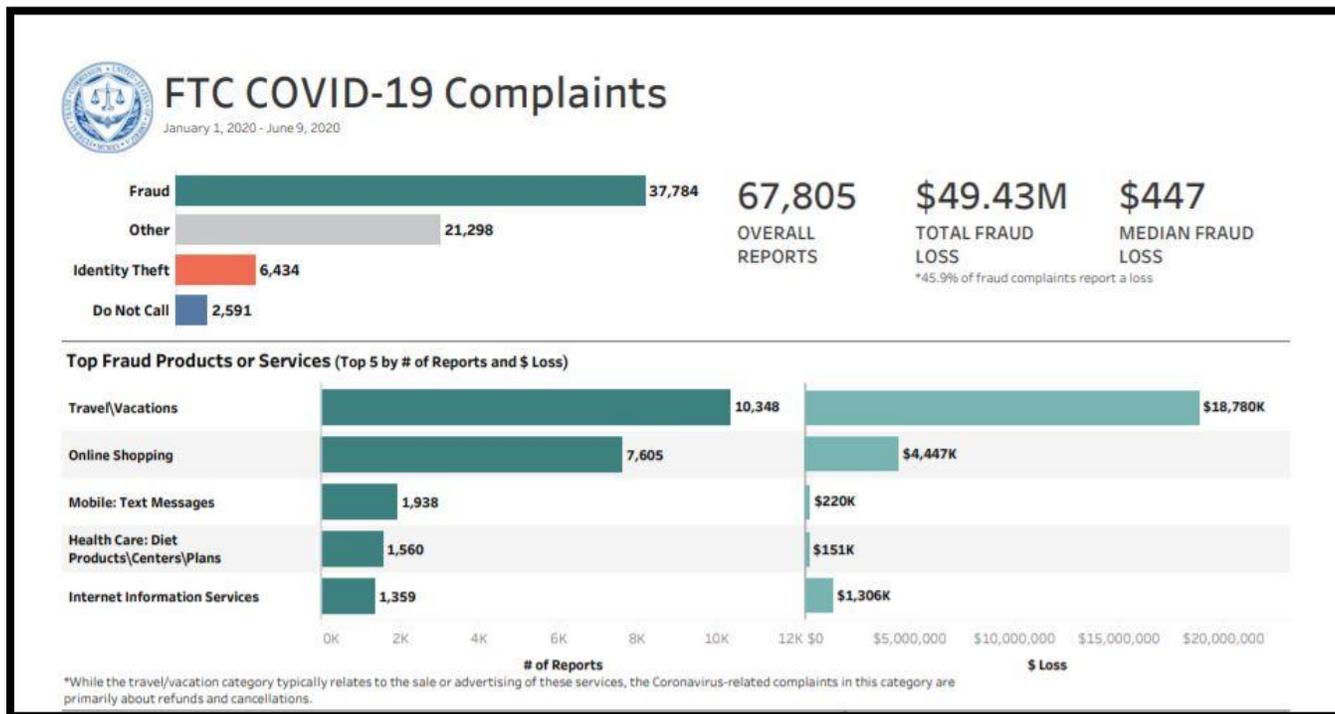


Figure 1 FTC Coronavirus Enforcement Webpage

(U) Utah COVID Fraud Cases

- (U) Emails and Texts
 - (U//LES) In April 2020 phishing emails were sent to approximately 30 municipal accounts in Washington state and one Utah state employee email. The malicious emails were made to look like a Department of Health official correspondence with a link to official Center for Disease Control information.
 - (U//LES) On 20 April, 2020, a malicious cyber actor posing as a University of Utah professor emailed students offering employment during the COVID-19 pandemic.
 - (U//LES) In March 2020, several scams involving COVID medical supplies, a COVID cure, and COVID financial relief emerged via email and text message from malicious actors.
- (U) Websites and Cell Phone Applications
 - (U//LES) A malicious Android cell phone application was used to distribute ransomware. Users would download the app believing they were receiving a COVID-19 heatmap but instead malicious actors would encrypt the user's phone and demand \$100 in exchange for decryption.
 - (U//LES) A malicious website pretending to be a COVID-19 tracking website infects visiting users with the AZORult trojan, an information stealing program.
 - (U//LES) On 3 March 2020, unknown cyber actors registered Coronavirusutah[.]com. The website currently hosts no content, but is insecure and will likely be used for typosquatting purposes. A typosquatting site could be used for malware distribution, phishing, credential harvesting, or host misinformation.

- (U) Counterfeit Products and Price Gouging
 - (U//LES) The Salt Lake City branch of the Federal Bureau of Investigation reported an increase in complaints regarding counterfeit COVID protective gear, test kits, and treatments.
 - (U//LES) A U.K. national was charged with shipping unapproved COVID-19 ‘treatment’ kits to California and Utah. Between 300 to 400 of the unapproved ‘treatment’ kits were shipped to a local Utah woman for around \$50 each. The woman gave many of the kits away but sold some for approximately \$200 each. Kits were shipped to both Ogden and Draper where the U.K. suspect has connections.
 - (U//LES) Homeland Security Investigations (HSI) received information that GENTOX MEDICAL SERVICES LLC located in Salt Lake City, was advertising the sale of N95 masks in a possible price gauging scheme. HSI Salt Lake City will open this case to further investigate and determine whether the company is in violation of 50 USC 4512 or 4513 Hoarding/Price Gouging of Designated Scarce Materials.

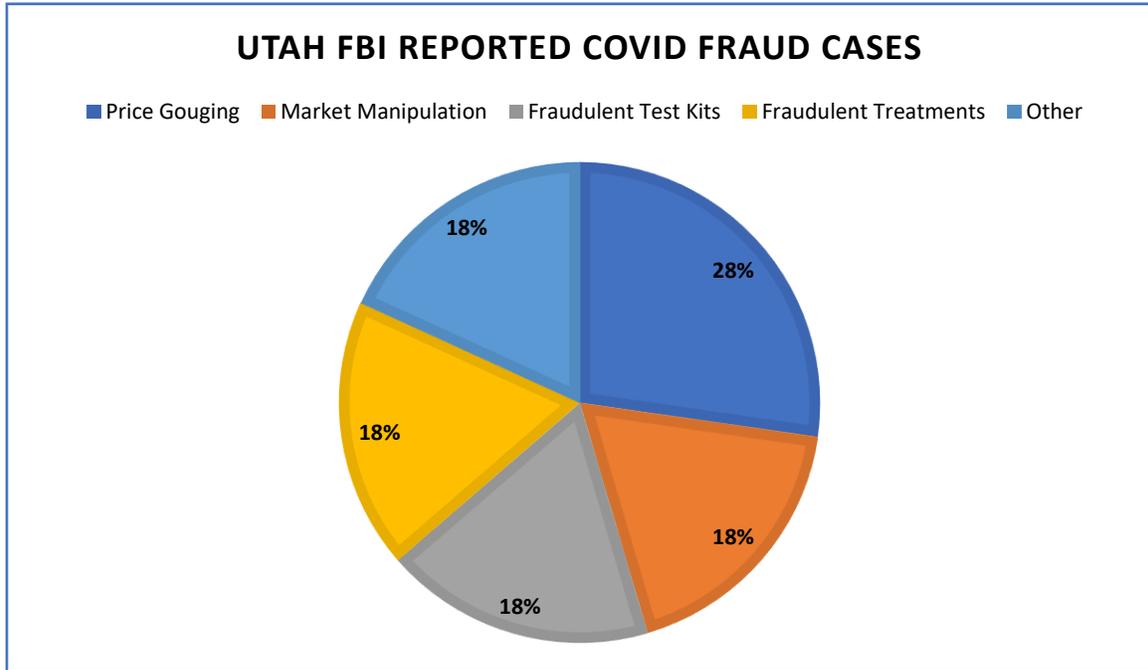


- (U) Social Media
 - (U//LES) A victim of fraud submitted \$35 for a processing fee solicited via Twitter to apply for financial aid due to COVID-19. The victim had their Instagram and Facebook account hacked and money was withdrawn from their bank account. The hacker then shifted to using the social media profiles to solicit funds from family/friends claiming the family had coronavirus.

(U) Federal Reports

(U//LES) The United States Attorney’s Office (USAO), Utah Division, reports 12 active COVID fraud cases. Although these cases cannot be prosecuted at this time due to courts being closed, the USAO anticipates being able to prosecute when courts are back in session.

(U//LES) The FBI's Salt Lake City division reported several COVID fraud cases beginning in January 2020 until the date of this report.



(U) Outlook

(U//LES) The SIAC assesses that COVID related fraud crimes will likely continue. The SIAC also assess that there will likely be an increase in COVID related fraud as the pandemic continues. Methods of fraud such as fraudulent test kits and malicious emails containing ransomware will continue to be utilized while incidences of price gouging may decrease as supplies rebound from their depleted state.

(U) Contact Information

(U//FOUO) Direct any questions or information regarding this subject to the Utah Statewide Information and Analysis Center via phone at 801-965-3838 or email at siac@utah.gov.

This report addresses DHS HSEC codes:
This report addresses SIAC Standing Information Requirements:

Attention: "Receipt of this information constitutes acceptance of all terms and conditions regarding its use, handling, storage, further dissemination or destruction. At a minimum, recipient acknowledges a commitment to comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information."

Handling Notice: Recipients are reminded that Utah Statewide Information and Analysis Center intelligence products may contain sensitive information meant for use primarily within the law enforcement and homeland security communities. Such products shall not be released in either written or oral form to the media, the general public, or other personnel who do not have a valid need-to-know without prior approval from an authorized Statewide Information and Analysis Center official. Unlawful dissemination of this information may adversely impact ongoing investigations, and thereby compromise law enforcement officers' safety and the safety and welfare of the public.