Medical Scams Related to COVID-19

By: Suzanne Rosenthall, CAMS

On May 18, 2020 FinCEN issued advisory FIN-2020-A002 to alert financial institutions to medical scams related to the COVID-19 Pandemic. The advisory addresses several different types of scams, as noted below.

Medical Related Frauds, Including Fraudulent Cures, Tests, Vaccines & Services

Examples of this type of fraud include claims related to purported vaccines or cures for COVID-19, claims related to products that purport to disinfect homes or buildings, and the distribution of fraudulent or unauthorized at-home COVID-19 tests. Red flags include, but are not limited to:

- The customer engages in transactions to or through personal accounts related to the sale of medical supplies
- Product branding images found in an online marketplace appear to be slightly different from the legitimate product's images
- A merchant requests payments that are unusual for the type of transaction or for the industry's pattern of behavior. For example, a merchant may require a pre-paid card rather than a credit card
- Financial institutions might detect patterns of high chargebacks and return rates indicative of merchant fraud

Non-Delivery Fraud of Medical-Related Goods

Disruptions to global shipping has created sudden demands for essential goods. Criminals may defraud customers through non-delivery of goods where a customer pays for merchandise that they never receive. Victims may include businesses, hospitals, governments, and consumers. These transactions may occur through websites, robocalls, or even the Darknet. Some schemes involve the use of shell companies. Red flags include, but are not limited to:

- The merchant does not appear to have a lengthy corporate history, lacks physical presence or address, or lacks an EIN.
- Listings in corporate databases contain vague or inappropriate names, multiple unrelated names, or multiple DBA names.
- The financial institution does not understand the merchant's business model and has difficulty determining the true nature of the company and its operations.

Price Gouging and Hoarding of Medical-Related Items

Hoarding and price gouging are defined as the act by any person or company of accumulating an unreasonable amount of any of these materials for their personal use, or for the purposes of selling surplus items far above prevailing market prices. These goods may include masks, disposable gloves, disinfectants, hand sanitizers, and toilet paper. Payment methods can vary and can include the use of pre-paid cards, credit card transactions, wires, or electronic fund transfers. Red flags include, but are not limited to:

- A customer uses their personal account for business purposes after January 2020 and sets up a medical supply company selling highly sought-after goods.
- A customer begins to use their money services or bank differently than they did prior to January 2020. For example, the customer begins to receive deposits with payment messages indicating they are for the sale of medical goods.
- The customer makes unusually large deposits that are inconsistent with their profile or account history.

FinCEN requests that financial institutions reference this advisory by including the key term "COVID19 FIN-2020-A002" in SAR field 2 (Filing Institution note to FinCEN) and that the narrative indicate a connection between the suspicious activity and the activities reported in the advisory. Financial institutions should also include the type of fraud and/or name of the scam or product (e.g., Product Fraud – non delivery scam) in SAR field 34(z). Refer to FinCEN's notice Related to the Coronavirus Disease 2019 May 18 Notice Related to COVID 19 which contains information regarding reporting COVID-19 related crime.

Click here for more information and a more complete list of red flags.