Banks May Need To Update Policies To Fight COVID-19 Fraud

By **Jennifer Achilles and Alejo Cabranes** (June 16, 2020)

Jennifer Achilles

Alejo Cabranes

During the COVID-19 pandemic, many financial institutions are already stretched thin navigating the small business loan programs under the Coronavirus Aid, Relief and Economic Security, or CARES, Act and responding to pandemic planning guidance issued by the Federal Financial Institutions Examination Council. Now the government also expects financial institutions to be the "first line of defense" in combating fraud schemes connected to the COVID-19 pandemic.[1]

On May 18, the Financial Crimes Enforcement Network issued its first COVID-19-related advisory to alert financial institutions to the types of medical fraud emerging during the pandemic.[2] The advisory is intended to help the financial industry identify red flags accompanying the most common types of fraudulent conduct currently occurring in the medical field.

The advisory is the first of many that FinCEN will be issuing in the coming weeks. Financial institutions will be expected to study these advisories, and to modify and/or tighten their compliance practices and procedures accordingly to be sure they are meeting their obligations under the Bank Secrecy Act.

Medical Fraud Identified During the Pandemic

According to the advisory, there are three primary types of medical fraud related to the COVID-19 pandemic: (1) fraudulent cures, tests, vaccines, and services; (2) nondelivery scams; and (3) price-gouging and hoarding of medical-related items, including personal protective equipment.

The advisory employs four real-life case studies that financial institutions may find helpful as they seek to identify COVID-19-specific risk factors and work to comply with their BSA reporting requirements. These four real-life cases studies depict a high degree of interagency coordination and collaboration across the federal government when it comes to medical fraud arising out of the COVID-19 pandemic.

1. Fraudulent Cures, Tests, Vaccines and Services

FinCEN wants financial institutions to be on the lookout for schemes involving fraudulent cures, tests, vaccines and associated services being offered to the public. The advisory highlights two recent cases in this category, both of which led to criminal charges being filed.

In mid-March 2020, U.S. Customs and Border Protection agents at LAX intercepted fake COVID-19 test kits that had arrived in the U.S. from the U.K., which triggered a joint U.S.-U.K. investigation and resulted in one arrest, the seizure of 300 additional kits, and over five gallons of chemicals used in the production of such kits. In a separate case from early April 2020, the U.S. Department of Justice charged a U.K. citizen with shipping mislabeled drugs that fraudulently purported to be COVID-19 treatments.

Although it is not clear whether financial institutions played a role in identifying the two cases discussed in the advisory, the advisory alerts financial institutions to eight "financial indicators" of these types of scams. For example, if a customer is engaging in the sale of medical supplies through personal accounts, or showing high chargebacks and return rates in their accounts, or has been identified by government agencies as selling fraudulent products, that may indicate activity that could trigger a SAR filing.

FinCEN clearly expects financial firms to incorporate additional measures into its KYC regime such as reviewing COVID-19 warning letters issued by the U.S. Food and Drug Administration, the Federal Trade Commission and the DOJ, conducting web-based searches of customer advertisements, and evaluating whether sales are being conducted at deep discounts or at highly inflated prices.

2. Nondelivery Fraud of Medical-Related Goods

In its advisory, FinCEN also highlights a financial institution in Virginia that alerted law enforcement to suspicious activity and helped prevent a $317 million nondelivery fraud. In that case, a foreign government asked a New York-based law firm for help procuring millions of N95 masks. The law firm contacted a broker (Company A), which in turn reached out to Company B, which claimed it possessed 50 million N95 masks, which were stored in a Texas warehouse, and requested a $317 million payment. Through the law firm, the foreign government initiated a wire transfer to a bank account held by Company A.

But the bank became suspicious and contacted the United States Secret Service because the account was opened the day before and Company A had never mentioned expecting a $317 million wire. Further investigation revealed Company A was a victim in the $317 million nondelivery scheme perpetrated by Company B, whose CEO later admitted there were never any masks.

FinCEN's advisory identifies nine red flags that are "financial indicators" of such nondelivery scams. These include when customers fail to provide documentation and information, as well as discrepancies between information provided by the customer and the results of a public record search. Financial institutions are expected to seek significant documentation from customers and apply a healthy dose of skepticism if they do not get it. Financial firms are also expected to perform their own searches in public records and corporate databases and review the data for discrepancies.

3. Price-Gouging and Hoarding of Medical-Related Items

The third type of medical fraud identified by FinCEN is price-gouging and hoarding of PPE. In late March 2020, the FBI arrested an individual for lying to agents about his hoarding and sale of surgical masks and other PPE. The individual told the FBI he worked for a company that buys and sells PPE materials "on an as-needed basis."

The FBI investigation revealed he had sold 1,000 N95 masks and other medical supplies to a pair of medical professionals at a 700% markup. When questioned by the FBI, the individual denied having possession of such materials in large, warehouse quantities. However, according to the criminal complaint, one of the medical professionals who picked up the purchased medical supplies from a local warehouse linked to individual, told FBI agents the warehouse contained enough medical supplies to "outfit an entire hospital."

The advisory highlights five additional red flags that could alert financial institutions to this type of fraud. For example, in the case highlighted above, a quick web-based search would

have presumably revealed that the individual did not work for a company that specialized in supplying medical supplies.

Financial institutions should also consider whether their customers are engaging in transactions for COVID-19-related goods involving companies outside of the medical industry; engaging in transactions related to the sale of medical supplies conducted through personal accounts; or receiving large deposits in connection with COVID-19-related medical supplies that are potentially inconsistent with a customer's account history.

Conclusion

The advisory showcases three primary types of medical fraud and 22 red flags that financial institutions should review to help identify them. FinCEN introduced the advisory as an effort to assist financial institutions, but this is not the kind of help that can be ignored. Given the sharp rise in COVID-19-related frauds, and the significant attention these frauds are receiving from the government, financial institutions should think critically about how best to incorporate the lessons learned in the advisory into their existing transaction monitoring systems and compliance policies.

Financial institutions are essentially being deputized to detect these specific types of schemes, and will be expected to modify or tighten their compliance policies to do so. While it is true that U.S. banking laws and regulations have increasingly brought the financial industry into partnership with the government, the advisory adds to the already heavy load of compliance personnel and programs.

Jennifer Achilles is a partner and Alejo Cabranes is an associate at Reed Smith LLP.

[1] Prepared Remarks of FinCEN Director Kenneth Blanco, NYU Law Program on Corporate Compliance and Enforcement (June 12, 2019) (urging audience members to consider "how compliance – by financial institutions in particular – plays a critical role in preventing these bad things from happening. In many instances, they are the first line of defense").

[2] FinCEN Advisory FIN-2020-A002 , "Medical Scams Related to the Coronavirus Disease 2019 (COVID-19)," (May 18, 2020).