FINCEN ADVISORY PUTS FINANCIAL INSTITUTIONS ON NOTICE FOR RED FLAGS INDICATIVE OF COVID-19-RELATED HEALTH CARE FRAUD

As the COVID-19 pandemic continues, health care firms and financial institutions are particularly at risk of becoming the subject of pandemic-related enforcement investigations. Because of their role in disbursing government stimulus funds and in processing customer transactions, financial institutions are also expected to identify potential indicators of pandemic-related fraud involving the health insurance and health care industries. On February 2, 2021, the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN") laid out numerous red flags in its *Advisory on COVID-19 Health Insurance- and Health Care-Related Fraud* ("Advisory") and directed financial institutions to be on the lookout for these scenarios.

HEALTH INSURANCE AND HEALTH CARE-RELATED FRAUD IN A PANDEMIC ENVIRONMENT

The Advisory makes clear the fraud schemes being used to take advantage of the pandemic environment are simply variations on standard health care fraud; opportunists are "adapting known health insurance and health care fraud to take advantage of the pandemic." The Advisory identifies seven representative categories:

- Unnecessary Services (unnecessary tests, often ordered in conjunction with COVID-19 tests, or tests for services that the company does not normally render);
- Billing Schemes (overbilling for COVID-19-related services or billing for services not actually rendered);
- Kickbacks (paying service providers or purported marketing organizations an illegal kickback or bribe "in exchange for ordering, or arranging for the ordering of, services and testing");
- Health Care Technology Schemes (false and fraudulent representations about COVID-19 testing, treatments, or cures "used to defraud insurance carriers and to perpetrate fraud on the financial markets by defrauding investors");

- Telefraud and Telehealth Schemes (collecting personally identifiable information ("PII"), through requests that are often linked to COVID-19 treatment or prevention, and "submit[ting] fraudulent claims for payment to health care benefit programs" or "submit[ting] fraudulent telehealth services claims");
- Fraudulently Obtaining COVID-19 Health Care Relief Funds (filing false claims and applications for federal relief funds provided under, e.g., the CARES Act, Paycheck Protection Program and Health Care Enhancement Act ("PPP-HCEA"), and the Economic Impact Disaster Loan program, where "the claim or application has a nexus to health care benefit programs"); and
- Identity Theft Leading to Additional Fraud (targeting beneficiaries for their PII and then using the stolen PII "to commit COVID-19-related fraud against health care benefit programs").

RED FLAGS FOR HEALTH INSURANCE- AND HEALTH CARE-RELATED FRAUD

The Advisory identifies red flags that should alert financial institutions to health insurance and health care-related fraud and "assist financial institutions in detecting, preventing, and reporting suspicious transactions related to such COVID-19-related fraud. These red flags fall into four categories: *"[a]dditional, medically unnecessary services or billing schemes," "[p]otential fraudulent businesses," "[k]ickbacks and money laundering," and "[f]raudulently obtaining COVID-19-relief funds*."

Additional Medically Unnecessary Services or Billing Schemes

Because many businesses have experienced a reduction in client or patient volume as a result of the COVID-19 pandemic, the Advisory recommends that financial institutions look for health care benefit or insurance payments that are (a) higher than expected in light of "the provider's estimated business transactions" or "an expected diminished activity level during the public health emergency"; or (b) outside of "the expected type or volume of service" based on the specific characteristics of the business. Moreover, financial institutions should also be alert for instances where the business accounts of a provider of COVID-19-related health care services contain personal or medically irrelevant transactions.

Potential Fraudulent Businesses

The Advisory further emphasizes that financial institutions should pay close attention to changes in customer activity after the Secretary of Health and Human Services' declaration of a public health emergency on January 31, 2020, and in particular accounts that began "receiving steep increases in health care benefit program or health insurance payments" after the declaration. Financial institutions should also look for evidence of a lack of "actual business activity" (e.g., accounts that "do[] not receive small-dollar check deposits, payments from merchant fee services, or cash payments from patients that would indicate patient co-payments"). More generally, FinCEN alerts financial institutions to be watchful for businesses that were seemingly created expressly for the purpose of obtaining COVID-19 funds or other government health care funds. Indicators of this type of fraud include

businesses without an internet presence or with incongruous (or nonexistent) physical locations.

The Advisory also includes a case study involving a sham business run out of New York in which the defendants hired pharmacists to pretend to work at fictional pharmacies so that they could fraudulently bill Medicare, but in reality these pharmacies never had any real prescriptions to fill or dispense.

Kickbacks and Money Laundering

The Advisory warns financial institutions to be wary of accounts that suddenly became more complicated after the pandemic, as "overly complex, medical-related transactions involving multiple counterparties" could be "indicative of possible structuring, layering kickbacks, or fraudulent medical claims." Financial institutions should also pay attention to unusually large advertising or market-related expenditures, and health care service providers that receive payments from health care service companies or laboratories without corresponding financial documentation.

Fraudulently Obtaining COVID-19 Relief Funds

FinCEN's Advisory also directs financial institutions to be on the lookout for "unexpected or excessive" COVID-19-related payments to accounts that were not previously associated with the provision of health care services, particularly in instances where the funds are withdrawn shortly after they are deposited, or to accounts that *were* previously associated with the provision of health care services but that have not been recently active or appear to be defunct. The Advisory also warns of account holders who simultaneously receive COVID-19-related unemployment insurance payments as well as substantial amounts of reimbursements from health care benefit programs or health insurance companies for services rendered.

CONCLUSION

FinCEN's Advisory is yet another reminder that financial institutions are on notice that they are expected to monitor red flags that are potential indicators of health care fraud in a pandemic environment. While one red flag alone is rarely indicative of fraud, FinCEN emphasizes that financial institutions should evaluate all other relevant factors involved in a customer's business when red flags are present. As in all industries, financial institutions should be particularly mindful with respect to third-party vendors.

FinCEN further directs financial institutions that identify the type of behavior described in the Advisory to file suspicious activity reports ("SARs") that include the Advisory's key term, "FIN-2021-A001." Additional instructions for filing SARs can be found in the Advisory. Financial Institutions should continue to be mindful of the government's increasing expectations that they are expected to play a key role in the monitoring and detection of COVID-19-related fraud schemes. Compliance systems, processes, and personnel should all be reviewed and, if necessary, enhanced, to ensure that resources are commensurate with the government's expectations in this climate.

CONTACTS

David DiBari
Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Joshua Berman
Partner

T +1 202 912 5174
E joshua.berman
@cliffordchance.com

Glen Donath
Partner

T +1 202 912 5138
E glen.donath
@cliffordchance.com

Steve Nickelsburg
Partner

T +1 202 912 5108
E steve.nickelsburg
@cliffordchance.com

Michelle Williams
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Philip Angeloff
Counsel

T +1 202 912 5111
E philip.angeloff
@cliffordchance.com

Christine Chen
Associate

T +1 202 912 5081
E christine.chen
@cliffordchance.com

Anna Mount
Associate

T +1 202 912 5052
E anna.mount
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Bangkok • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Doha • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • Jakarta* • London • Luxembourg • Madrid • Milan • Moscow • Munich • New York • Paris • Perth • Prague • Rome • São Paulo • Seoul • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.