New York Law Journal
White-Collar Crime
WWW.NYLJ.COM
An ALM Publication
JUNE 25, 2021

WHITE-COLLAR CRIME

COVID-19 Fraud Schemes Rise Amid Pandemic

BY ROBERT APPLETON

Amongst the various unexpected consequences of the pandemic, the last 16 months have ushered in an increased wave and new level of sophistication of fraud schemes, as well as adaptions to the traditional modus operandi of perpetrators, including the expanded use of technology and digital means as a favored medium during the period of social distancing and quarantine.

As of June 3, the FTC had logged nearly 536,000 consumer complaints related to COVID-19 and stimulus payments, more than 71% of them involving fraud or identity theft, with an estimated cost of more than $464 million in losses. In 2020, the number of fraud, identity theft, and other related reports to the FTC increased more than 45% from approximately 3.12 million to 4.72 million, and reported losses from fraud grew from $1.8 billion in 2019 to more than $3.3 billion in 2020.

In addition to the common and traditional fraud schemes, COVID-19 has triggered twists and modifications, such as deceptive claims by marketers for COVID-19 related products and services claiming to address demand for scarce goods, peddling treatments and cures, offering to alleviate financial distress from the pandemic, as well as efforts to "help" recipients expedite the receipt or maximize the use of COVID-19 relief funds. Simultaneously, the period ushered in a new wave of more sophisticated and targeted scams, through the use of digital technology, the Internet and cell phones, with a corresponding increase in both the volume and level of sophistication of such efforts.

In anticipation of a focus by perpetrators preying on those affected by the pandemic, Congress passed the COVID-19 Consumer Protection Act (CCPA) as part of the 2021 Consolidated

Appropriations Act that made it "unlawful … for any person … to engage in a deceptive act or practice … associated with the treatment, cure, prevention, mitigation or diagnosis of COVID-19 or a government benefit related to COVID-19." It did not take long for the government to bring the first case under the Act. On April 27, 2021, the Department of Justice brought charges under the CCPA against a St. Louis-based chiropractor and his company alleging defective marketing of products claiming that Vitamin D and Zinc as scientifically effective to treat or prevent COVID-19, and as being equally or more effective than presently available pandemic vaccines. While there has long been a focus on deceptive

ROBERT APPLETON *is a partner in the white-collar defense and government investigations practice at Olshan Frome Wolosky. He is a cross-border specialist and a former senior prosecutor in the U.S. Department of Justice.*

marketing, the pandemic has resulted in an increase in the number of cases being brought, as well as the regulatory response of new tools, such as the CCPA.

The timing of the passage of the CCPA takes on an increased importance, as the statute provides for civil monetary penalties for violations of the Act. Almost simultaneously as the first charges were being brought under the CCPA, on April 22, 2021 the U.S. Supreme Court decided the case of AMG Capital Management v. Federal Trade Commission (FTC) (No. 19-508 U.S. Supreme Court April 22, 2021). In the AMG Capital case, the Supreme Court invalidated the Commission's longstanding use of §13(b) of the FTC Act in consumer protection cases to obtain monetary judgments against defendants engaging in deceptive consumer practices. In the decision, the Supreme Court limited the FTC to purely enjoin fraudulent or deceptive commercial activity without first exhausting certain administrative processes. Normally, such a decision would be a significant setback to the enforcement community in deceptive trade practices cases. However, the decision should have minimal impact given the monetary remedies provided for by the CCPA, effectively serving as a substitute to the FTC Act in the government's arsenal.

While the government's efforts to address deceptive commercial conduct is by no means new, the CCPA gives the federal government additional tools against such misconduct, and to achieve monetary recoveries against the actors. So far, the statute has not yet proved an effective deterrent, however, given the skyrocketing number of allegations and referrals.

The reported data thus far, as well as our own experiences in such cases, shows that the pandemic has brought new COVID-related adaptions to more traditional fraud conduct as well as a shift in the nature, types and sophistication of the fraud schemes that are being perpetrated. From our own practice, we are seeing emerging trends: from new deceptive health and safety claims to new offers to capitalize on economic distress to new trends in the digital/Internet space. Advanced fee schemes have taken on COVID-related modifications.

With consumers facing skyrocketing unemployment rates and widespread financial anxiety, the FTC reported that complaints to them of income-related scams "reached the highest levels on record in the second quarter of 2020." See FTC Consumer Protection Data Spotlight, Income Scams: big promises, big losses (Dec. 10, 2020). Identity thieves honed in on unemployment benefits. The FTC reports that in 2020 over 394,000 reports were submitted by individuals who claimed that their information was "misused" to apply for a government benefit in their name. This number represents a 3,000% increase from 2019. See Protecting Consumers During the COVID-19 Pandemic: The FTC: A Year in Review, at page 4. In response, the FTC created Operation Income Illusion, a December 2020 effort by the FTC with some 19 other law enforcement partners. Already, the Task Force has generated more than 50 law enforcement operations. Working in cooperation with the DOJ, the FTC launched an Unemployment Insurance page on IdentityTheft.gov to educate the public on where and how consumers can protect their credit.

Similarly, we have seen an uptick and have represented clients in phishing scams and robocalls where purported vendors offer to sell medical devices, such as masks or respiratory equipment, with no intention to deliver the products. (Phishing is the fraudulent practice of sending emails purportedly from a reputable source to induce individuals to reveal personal information, such as passwords, credit cards numbers and/or social security numbers). The DOJ confirms such an increase in its "Report Covid-19 Fraud," posted on its website. These schemes are an offshoot of the age-old tactic of advance payment schemes, namely efforts to persuade the victim to make a payment in advance to secure a product, service or an opportunity, or a much larger payment in return.

Advanced payment schemes, one of the most popular and traditional forms of fraud, have taken modified twists and turns with the pandemic. We have seen, and DOJ has reported, a number of cases related to the overpayment of stimulus money. In these schemes, the victim receives a call that he/she obtained a mistaken overpayment of stimulus monies and the caller, posing as a representative from the government, demands a refund via WesternUnion or MoneyGram, or even a stored value card. See Dep't of Justice, Report COVID-19 Fraud (updated March 11, 2021). DOJ also reports that it has seen an increase in social media scams and electronic (telephone or text) outreach fraudulently seeking donations for non-existent charities to be made through the transmission of bank account information online. Emails and texts refer to a link to download that could be an effort to infect the recipient's device with malware or malicious software to purloin personal information. Id.

According to FinCEN, the Treasury Department's Financial Crimes Enforcement Network, the pandemic has brought with it "significant broad based and targeted phishing campaigns." According to FinCEN, tens of thousands of new websites have been created and domain names registered with the terms related to the pandemic. The DOJ says that it has shut down hundreds of such sites and that hundreds of cybercriminals that have "sought to rip people off during the pandemic have had their websites busted." According to the U.S. Secret Service, many sites tried to attract traffic using domain names with words such as "covid19" or "coronavirus."

Scammers have re-tooled some of the more traditional schemes to fit the pandemic. According to Scott Moritz, Senior Managing Director at FTI Consulting, "fraudsters have successfully reframed Business Email Compromise schemes in a COVID-19 wrapper." Moritz has seen two types of BEC schemes: one, a "Fake Executive Scheme" and two, an "Accounts Payable Compromise" scheme. In the Accounts Payable Compromise scenario, the scheme relies upon the compromise of email or network credentials of employees who receive vendor invoices and are responsible for payments. The scammers compromise and then harvest the inboxes of these employees for invoices, alter the payment instructions and either re-send the invoice or call the company as the vendor and provide new payment instructions. In the Fake Executive scheme, the fraudsters collect information on the company and its senior executives and identify the employee(s) with wire transfer authority. Then, they either spoof an email account of a senior executive to induce the lower-level employee with wire authority to send an urgent wire for a COVID-related purpose, either to secure PPE, test kits or vaccines. According to Moritz, these schemes have seen an uptick and have combined to cause staggering losses.

In all, it remains to be seen whether these schemes are here to stay or will be replaced by even newer methods as the pandemic wanes. One thing is for sure, the pandemic has ushered in greater use of digital means in fraud schemes, and an increase in cross border fraud, triggering an urgent need to be vigilant, proactive and sensitive to such efforts, initiate relevant controls, and take prompt action when red flags of fraud emerge.

Robert M. Appleton
212.451.2288

RAppleton@olshanlaw.com