THOMSON REUTERS
Westlaw®

Section 1028A: Potent weapon in fight against COVID-19 related fraud

By Michael Glenn, Esq., Brian Hayes, Esq., and Jeremy Sternberg, Esq., *Holland & Knight LLP*

JULY 8, 2020

The passage of the Coronavirus Aid, Relief, and Economic Security Act (Cares Act) and the unprecedented $2-trillion economic stimulus package it established provides fertile opportunity for bad actors to engage in fraud.

The history of prior emergency stimulus packages, such as the Hurricane Katrina relief funds, demonstrates that there will be an inevitable increase in investigations and enforcement actions as the funds are disbursed and spent and the country emerges from the current economic crisis.

> The federal aggravated identity theft statute, 18 U.S.C.A. § 1028A, can be expansively applied by federal prosecutors across many different factual scenarios.

In fact, since the early days of the coronavirus pandemic, the U.S. Department of Justice (DOJ) has taken an aggressive stance against those seeking to exploit the ongoing global health crisis through fraudulent and otherwise illegal schemes.

On March 16, 2020, U.S. Attorney General William Barr directed every U.S. Attorney's Office to prioritize the detection, investigation and prosecution of all criminal conduct related to the COVID-19 crisis.[1]

In a follow-up memorandum, Deputy Attorney General Jeffrey Rosen highlighted a variety of reported schemes emerging from the pandemic and emphasized several tools currently available to federal prosecutors to deal decisively with the alleged criminal schemes.[2]

A CLOSER LOOK AT THE AGGRAVATED IDENTITY THEFT STATUTE

One such tool the government has already employed — and is likely to continue to look for opportunities to deploy — is the federal aggravated identity theft statute, 18 U.S.C.A. § 1028A, established through the enactment of the Identity Theft Penalty Enhancement Act (ITPEA) in July 2004.

According to the Act's legislative history, Congress was frustrated that "many identity thieves receive short terms of imprisonment or probation" and "after their release, many of these thieves will go on to use false identities to commit much more serious crimes."[3]

The statute imposes a mandatory minimum two-year sentence enhancement if the government proves that the defendant "during and in relation to" certain predicate felony offenses "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person."[4]

The wide variety of predicate offenses highlights that 18 U.S.C.A. § 1028A can be expansively applied by federal prosecutors across many different factual scenarios.

Moreover, the statute broadly defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[5]

By way of brief background on the statute and its application, the U.S. Supreme Court held in *Flores-Figueroa v. United States,* 556 U.S. 646 (2009), that the statute requires the government to show that the defendant knew that the means of identification at issue belonged to another person to satisfy the *mens rea* requirement.[6]

Since then, the U.S. Courts of Appeal for the First and Ninth Circuits have narrowly construed the "use" requirement of Section 1028A to reach only defendants who attempt to pass themselves off as the third party or purport to take an action on the third party's behalf.[7]

Notably, the enhanced penalty must be served consecutively to any other punishment imposed for another offense, including the underlying felony offense during which the aggravated identity theft occurred.

This enhanced penalty essentially insures at least a two-year prison sentence for anyone convicted of aggravated identity theft, and the U.S. Sentencing Commission statistics for 2019 demonstrate that in many cases the prison term will be much longer, as the average sentence for those convicted under Section 1028A was 47 months.[8]

Other key statistics from the Commission's FY 2019 report highlight the powerful and broad reach of the statute in the government's fight against identity theft.

First, 44.2% of offenders convicted under Section 1028A had *little or no prior criminal history*. Second, only in the rarest of circumstances (less than 3% of cases) did offenders receive a substantial assistance departure under Section 3553(e) from the two-year statutory minimum.

These statistics are a cautionary tale for those individuals attempting to capitalize on the pandemic through the misuse of the identification of another.

RECENT COVID-19 ENFORCEMENT ACTIONS INVOLVING THE AGGRAVATED IDENTITY THEFT STATUTE

Recent DOJ enforcement actions highlight the government's efforts to use this robust prosecutorial tool to combat coronavirus-related fraud.

> There likely will be an effort in investigations and audits related to CARES Act applications and funding to identify any potential misuse of a "means of identification."

On May 5, 2020, two New England businessmen, David Staveley and David Butziger, were the first to be charged with allegedly defrauding the CARES Act and the U.S. Small Business Administration's (SBA) $660 billion Paycheck Protection Program (PPP) that it established to assist businesses in retaining their employees during the economic shutdown.[9]

Specifically, Staveley and Butziger are charged with conspiracy to make a false statement and conspiracy to commit bank fraud in connection with over $500,000 in PPP loans they applied for on behalf of four different business entities for which there were no actual employees.

In addition to the conspiracy charges and a charge of bank fraud against Butziger, Staveley is charged with aggravated identity theft for allegedly using his brother's name and Social Security number to, among other things, apply for PPP stimulus funds.

On May 26, 2020, federal authorities announced the arrest of Richard Schirripa of Long Island, New York, a licensed pharmacist known as "the Mask Man," on charges of violating the Defense Production Act by hoarding and price gouging N95 masks, making false statements to law enforcement, committing healthcare fraud and aggravated identity theft.[10]

According to the allegations of the complaint, Schirripa engaged in at least three distinct criminal schemes:

(1) the hoarding and price gouging of N95 masks,

(2) lying to U.S. Drug Enforcement Administration officers, and

(3) causing Medicare and Medicaid to be billed for prescriptions based on false representations over a five-year period.

In connection with the healthcare fraud scheme, Schirripa is alleged to have used the personal identifying information of his pharmacy's patients, without their authorization, giving rise to the aggravated identity theft charge.

CONCLUSION AND CONSIDERATIONS

Although the government's enforcement of coronavirus-related fraud is just now ramping up, it is clear from the aforementioned actions that the government will use every means in its arsenal to prosecute those who seek to profit from fraudulent schemes as a result of the global pandemic.

While these current enforcement actions target apparently easy to detect fraudulent schemes early in the cycle, it will take time and significant investigative efforts for the government to detect, investigate, and prosecute more complex schemes. Armed with time and a special inspector general, such activity is inevitable.

Given the broad reach and severe penalties of Section 1028A, and the government's early use of the aggravated identity theft statute in a few coronavirus-related fraud cases already, there likely will be an effort in investigations and audits related to CARES Act applications and funding to identify any potential misuse of a "means of identification."

Paying scrupulous attention to the "means of identification" used in applications, certifications, and other documents associated with obtaining and using coronavirus-related relief funds should clearly be an important part of those processes.

Notes

[1] Memorandum from Attorney General William Barr to all U.S. Attorneys, COVID-19 – Department of Justice Priorities (March 16, 2020).

[2] Memorandum from Deputy Attorney General Jeffrey Rosen, Department of Justice Enforcement Actions Related to COVID-19 (March 24, 2020).

[3] H.R. Rep. No. 108–528, at 3 (2004), reprinted in 2004 U.S.C.C.A.N. 779, 780.

[4] 18 U.S.C.A. § 1028A. The statute lists 11 subsections of predicate felonies, including bank fraud, healthcare fraud, mail fraud, Social Security fraud and wire fraud. Id. § 1028A(c).

[5] 18 U.S.C.A. § 1028(d)(7).

[6] *Flores-Figueroa v. United States*, 556 U.S. 646, 657 (2009) ("We conclude that § 1028A(a)(1) requires the Government to show that the defendant knew that the means of identification at issue belonged to another person.")

[7] *See United States v. Hong*, 938 F.3d 1040, 1051 (9th Cir. 2019); *United States v. Berroa*, 856 F.3d 141, 156 (1st Cir. 2017).

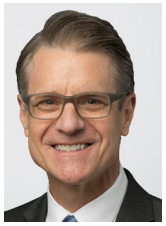
[8] U.S. Sentencing Commission, Quick Facts – Section 1028A Aggravated Identity Theft Offenses.

[9] Press Release, DOJ, Two Charged in Rhode Island with Stimulus Fraud (May 5, 2020).

[10] Press Release, DOJ, Licensed Pharmacist Charged With Hoarding and Price Gouging of N95 Masks in Violation of Defense Production Act (May 26, 2020).

This article appeared on the Westlaw Practitioner Insights Commentaries web page on July 8, 2020.

ABOUT THE AUTHORS


Michael Glenn (L) is an associate and **Brian Hayes** (C) and **Jeremy Sternberg** (R) are partners with **Holland & Knight LLP**. They are all members of the firm's White Collar Defense and Investigations Team. Glenn is located in the firm's Miami office and can be reached at michael.glenn@hklaw.com. Hayes is based in Chicago and can be reached at brian.hayes@hklaw.com. Sternberg is located in Boston. He can be reached at jeremy.sternberg@hklaw.com. This article reflects the situation at the time it was written based on the rapidly changing nature of the COVID-19 pandemic.