U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

June 12, 2021

BY ECF AND HAND DELIVERY

The Honorable Jed S. Rakoff
United States District Judge
Southern District of New York
500 Pearl St.
New York, New York 10007

Re: *United States v. Hamid "Ray" Akhavan*, S3 20 Cr. 188 (JSR)

Dear Judge Rakoff:

The Government respectfully submits this letter in connection with the sentencing of defendant Hamid "Ray" Akhavan, scheduled for Friday June 18, 2021, at 11:00 AM.

Motivated by greed, Akhavan was the leader and mastermind of a massive payment processing scheme (the "Scheme") for a period of approximately three years. Akhavan, who was already a successful businessman, was paid millions of dollars in exchange for his criminal services. As the leader of the Scheme, Akhavan oversaw an international payment processing scheme that was designed to trick issuing banks in the United States and credit card companies into processing in excess of $150,000,000 in marijuana transactions that were disguised as lawful purchases. Akhavan's Scheme was difficult to detect, elaborate and complex—it involved the use of offshore bank accounts, phony webpages, online tracking pixels, and forwarded customer service phone numbers, which were all designed to conceal the scheme from banks, credit card companies, and law enforcement. Despite his awareness that he was under investigation by the FBI, Akhavan continued to operate the Scheme until it collapsed in 2019.

Undeterred by his arrest in the instant case, or his probation status on a state case in California, Akhavan also continued to engage in criminal conduct while on bail. Specifically, in the fall of 2020, Akhavan possessed two firearms, and a prescription bottle that appeared to contain crack cocaine. Akhavan's possession of firearms while on probation and on bail in this case is an egregious example of his complete lack of respect for the law.

In light of the seriousness of the defendant's crimes, and for all of the reasons set forth below, a substantial term of imprisonment, below the Guidelines range, would be sufficient, but not greater than necessary, to serve the legitimate purposes of sentencing.

Background

I. Offense Conduct

A. Overview of the Fraud Scheme

Akhavan and his co-defendant Ruben Weigand were charged and convicted in one count with participating in a conspiracy to commit bank fraud, in violation of Title 18, United States Code, Section 1349, from in or around 2016, through in or around 2019. Akhavan, working with others, including Weigand and principals from one of the leading on-demand marijuana delivery companies in the United States, named Eaze, planned and executed a scheme to deceive United States banks and other financial institutions into processing over one hundred and fifty million dollars in credit and debit card payments for the purchase and delivery of marijuana products. (PSR ¶ 17, Tr. 1430:21-1431:21). Because many United States banks, as well as Visa and MasterCard are unwilling to process payments involving marijuana products, Akhavan, Weigand, and other co-conspirators utilized the Scheme in order to avoid these restrictions and facilitate Eaze's credit and debit card processing. (PSR ¶ 18, Tr. 1430:4-20)

1. Background on Eaze

Eaze is a California-based company that arranged for the on-demand sale and delivery of marijuana products to customers located primarily in California. (PSR ¶ 19, Tr. 138: 1-7). Through Eaze's mobile application and website (collectively, the "Applications"), customers could order marijuana from different dispensaries. (PSR ¶ 19, Tr. 146:3-7). Specifically, customers used the Applications to select the marijuana product(s) of their choice, and to receive delivery of their selection shortly thereafter. (PSR ¶ 19, Tr. 147:4-14). Although Eaze operated the technology platform through which users purchased marijuana (i.e., the Applications), it was not the actual retailer of the marijuana. The actual retailers were the dispensaries, which contracted with Eaze to fulfill orders placed by customers through the Applications. (PSR ¶ 19, Tr. 138:8-10)

To request and receive a delivery of marijuana through the Applications, a user created an Eaze account through the company's website or mobile application. (PSR ¶ 20, Tr. 146: 24-147: 3). Once the customer selected his or her product(s) for purchase, the Application generated a check-out screen for the order where the customer could select a payment option. (PSR ¶ 20, Tr. 147: 5-9). At various points from in or around 2016, through in or around 2019, Eaze offered credit cards and debit cards as payment options. (PSR ¶ 20, Tr. 1441: 2-4). For purchases with credit cards or debit cards, the Applications allowed customers to enter their card information and then complete the payment using that information. (PSR ¶ 20, Tr. 147: 4-9).

Once a customer placed an order, a delivery driver would deliver the order to the customer shortly thereafter. (PSR ¶ 21, Tr. 147: 10-14). Once the delivery was complete, Eaze generated and transmitted via email a receipt for the purchase. (PSR ¶ 21, Tr. 147: 19-21). When customers made purchases by credit cards or debit cards, those purchases would appear on the customers' card statements. The information regarding the merchant name and location on the customer's card statement, however, would indicate that the purchase was made from a merchant other than

Eaze (e.g., a merchant from whom the customer had not in fact purchased the marijuana). (PSR ¶ 21, Tr. 159: 21-160:6)

2. Details of the Scheme

The Scheme involved the deception of virtually all of the participants in the payment processing network, including issuing banks in the United States (the "Issuing Banks") and Visa and MasterCard, through the use of fake merchant names, fake merchant locations, fake descriptions of the merchant activities, and fake merchant descriptors. (Tr. 1430: 7-17). There were far more than ten Issuing Banks that were victims of the defendants' Scheme. (PSR ¶ 22, GX 2201, 2202, 2301, 2302).

The primary method used by Akhavan, Weigand, and other co-conspirators to deceive the Issuing Banks involved the purchase and use of shell companies that were used to disguise the marijuana transactions through the use of phony merchants (the "Phony Merchants"). (PSR ¶ 23, Tr. 1442: 3-10). The shell companies were used to open offshore bank accounts with merchant acquiring banks and to disguise credit and debit card charges for marijuana purchases made through Eaze. (PSR ¶ 23, Tr. 1443: 3-6). In particular, Akhavan and Weigand worked with other co-conspirators to apply for and obtain the phony merchant accounts– including for phony online merchants purportedly selling dog products, diving gear, carbonated drinks, green tea, and face creams – and established Visa and MasterCard merchant processing accounts with one or more offshore acquiring banks. (PSR ¶ 23, Tr. 878: 17-879: 3). Many of the Phony Merchants purported to be based in the United Kingdom, but, despite being based outside of the United States, claimed to maintain U.S.-based customer service numbers. (PSR ¶ 24, Tr. 1364: 20-24; Tr. 827: 2-4). Akhavan and Weigand had insiders at some of these acquiring banks who were aware that the Phony Merchants were being used to process marijuana transactions and provided feedback on the merchant bank account applications for the Phony Merchants in order to ensure that the accounts were opened successfully. (PSR ¶ 24, Tr. 729: 17-24). Akhavan and Weigand then arranged for more than a dozen of the Phony Merchants, with their corresponding merchant bank accounts, to be used by Eaze to process debit and credit card purchases of marijuana products. (PSR ¶ 24, Tr. 1443: 18-21)

To assist in obtaining the phony merchant bank accounts, Akhavan and Weigand were provided access to a software program referred to as Webshield that was misused by the defendants in order to circumvent the merchant banks' compliance protocols. (PSR ¶ 25, Tr. 869: 3-7). Webshield is a company that provides legitimate merchant risk services that are designed to help acquiring banks assess the risks associated with merchants in their portfolio. (PSR ¶ 25, Tr. 868: 17-24). Webshield is often used during the onboarding process for new merchants who are applying for merchant bank accounts. (PSR ¶ 25, Tr. 868: 17-24). The defendants were provided with access to the Webshield tool by a co-conspirator named Christian Chmiel, who allowed them to misuse the tool in order to get around the risk assessment checks that were in place at acquiring banks. (PSR ¶ 25, Tr. 870: 1-10).

To facilitate the Scheme, webpages were created and deployed to lend legitimacy to the Phony Merchants, and to avoid detection of the Scheme. (PSR ¶ 26, Tr. 889: 1-11). The Phony Merchants typically had web pages suggesting that they were involved in selling legitimate goods, such as carbonated drinks, face cream, dog products, and diving gear. (PSR ¶ 26, Tr. 266: 10-22).

Yet these companies were actually used by the defendants to facilitate the approval and processing of marijuana transactions. (PSR ¶ 26, Tr. 1100: 16-19). Some of the merchant websites listed for those transactions included: diverkingdom.com, desirescent.com, outdoormaxx.com, and happypuppybox.com. (PSR ¶ 26, Tr. 470: 8-22). Moreover, none of the Phony Merchant website names listed for those transactions referred to Eaze or to marijuana. The defendants' scheme even involved fake visits to those websites to make it appear as though the websites had real customers and were operating legitimate online businesses. (PSR ¶ 26, Tr. 890: 7-11).

The defendants' scheme also involved the use of online tracking pixels. (PSR ¶ 27, Tr. 2254: 7-11). Because the descriptors listed on Eaze's customers' credit card statements often were the URLs for the Phony Merchant websites, Eaze's customers were sometimes confused and did not recognize the transactions on their credit card statements. (PSR ¶ 27, Tr. 1442: 14-24). The defendants and their co-conspirators were concerned that confused customers would call their Issuing Banks and inadvertently reveal the Scheme by indicating that they had purchased marijuana products and/or that they had made a purchase through Eaze. (PSR ¶ 27, Tr. 1465: 6-13). To lessen the risk that customers would be confused, the defendants used a number of techniques, including employing online tracking pixels to track which users had visited Eaze's website. (PSR ¶ 28, Tr. 2254: 7-11). If an Eaze customer who had visited Eaze's website then went to the URL listed on their credit card statement (i.e., the URL of a Phony Merchant), the tracking pixels would automatically re-route the customer to a webpage connected to Eaze so that the customer would understand what the real purchase had been for (i.e., from Eaze). (PSR ¶ 28, Tr. 1486: 22-1487:6). To hide the Scheme, the defendants ensured that third-parties who were not Eaze customers, such as bank or credit card company investigators, would not be re-routed, and would therefore be unable to discern any connection between the Phony Merchant website and Eaze and/or the sale of marijuana products. (PSR ¶ 28, Tr. 1486: 22-1487: 6).

Akhavan, Weigand, and others also worked with and directed others to apply incorrect merchant category codes ("MCCs") to the marijuana transactions in order to disguise the nature of those transactions and create the false appearance that the transactions were completely unrelated to marijuana. (PSR ¶ 29, Tr. 1577: 8-19). Some of the MCCs/categories listed for the transactions included freight carrier trucking, clock jewelry watch and silverware, stenographic services, department stores, music stores/pianos, and cosmetic stores. (PSR ¶ 29, Tr. 471: 18-22)

Over $150 million in marijuana credit and debit card transactions were processed using the Phony Merchants. (PSR ¶ 30, Tr. 280: 7).

There were two phases of the Scheme. The first phase of the Scheme operated from 2016 through in or around early 2018. This phase of the Scheme was generally referred to by the name "Clearsettle." (PSR ¶ 31, Tr. 1443: 7-11). The second phase of the Scheme, generally referred to by the name "EU Processing," became operational in or around April 2018, although plans for the second phase were underway earlier. (PSR ¶ 31, Tr. 1443: 16-17). For example, in or around January 2018, Weigand, Akhavan, and other co-conspirators met at Akhavan's office in Calabasas, California ("Akhavan's Office") for a meeting in which they discussed and planned the second phase of the Scheme. (PSR ¶ 32, Tr. 710: 5-11). In addition, Akhavan, Weigand, principals at Eaze and from the marijuana dispensaries, all met at Akhavan's Office in California in March 2018 to discuss and plan the second phase of the Scheme. (PSR ¶ 32, Tr. 1690: 15-20). Akhavan

participated in both phases of the Scheme. Weigand participated in the second phase of the Scheme. During the second phase of the Scheme, the Issuing Banks remitted approximately $108,320,268.20 as a result of the fraudulent misrepresentations conveyed to the Issuing Banks in furtherance of the Scheme. (PSR ¶ 33, GX 687).

During the first phase of the Scheme, Akhavan and his co-conspirators charged Eaze and the dispensaries a fee of approximately 8.75%. (PSR ¶ 34, GX 425). During the second phase of the Scheme, Akhavan and his co-conspirators charged the defendants a fee of approximately 12%. (PSR ¶ 34, Tr. 1327: 16-18)

3. Defendants' Roles in the Scheme

As described in more detail below, Akhavan was the leader of the Scheme and oversaw the entire operation. (PSR ¶ 35, Tr. 176, 710, 726-727, 730-731, 1445, 1560, 1838-39, 2254; GX 411, 417, 4004, 4002).

Weigand was recruited into the second phase of the Scheme by Akhavan. Weigand was responsible for the relationships with the overseas acquiring banks during the EU Processing phase of the scheme, including facilitating the applications for merchant bank accounts on behalf of the Phony Merchants, reviewing fraudulent applications prepared by co-conspirators (Tr. 729:8-24; GX 3968; GX 4004 at 3; GX 4002 at 3-5; GX 3940 & 3707), interfacing with the acquiring banks regarding the merchant bank accounts once they were established (Tr. 729:8-24; Tr. 1115:8-23; GX 302, at 10:52; GX 1802; GX 3935; GX 3923; GX 4004 at 4-7, 19-20, 83-87; GX 1722), and providing statements to the dispensaries regarding the flow of proceeds from the marijuana transactions back to bank accounts in the United States. (PSR ¶ 36, Tr. 2254: 21-23; GX 4004 at 65; GX 485, 1709, & 1801). Weigand also worked on forwarding customer service phone numbers connected to the Phony Merchants to Eaze. (GX 4004 at 39-40, 62-64). Ruben also directed other members of the Scheme, such as Oliver Hargreaves, to prepare application packages for particular banks, such as Kalixa, Wirecard, and E-Comprocessing. (Tr. 802:16-18).

Co-defendant and cooperating witness James Patterson began working for Eaze in approximately April 2016 as its Chief Product and Technology Officer. Patterson was promoted to CEO of Eaze in December 2016 and stayed in that position until late 2019. As CEO, Patterson was the primary point of contact on behalf of Eaze with Akhavan and Akhavan 's payment processing network.

Co-conspirator and cooperating witness Oliver Hargreaves was hired by Akhavan to prepare fraudulent application packages to submit to overseas banks, and to create webpages for Phony Merchants who were used in the Scheme.

II. Akhavan's Post-Arrest Conduct

In around November 2020, while released on bail on this case, Akhavan unlawfully possessed two firearms, one of which was loaded. On October 24, 2020, an officer with the Los Angeles Police Department ("LAPD") responded to an overdose radio call and found Akhavan being treated by the Los Angeles fire department for a drug overdose. Akhavan lied to the LAPD officer and told him that he was not on probation, even though he was then serving his term of probation in connection with his state convictions and was on pretrial supervision in connection with this matter. (PSR ¶ 41).

On November 5, 2020, LAPD officers conducted a probation compliance check at Akhavan's residence. During a search of his bedroom, they found two firearms—one of which was a loaded semi-automatic pistol, with a high-capacity magazine containing 12 rounds—and a prescription bottle that appeared to contain crack cocaine. *Id.* The guns were hidden inside of boxing gloves in a gym bag. The prescription bottle was also found inside of the gym bag. Akhavan claimed that the guns were not his—notwithstanding that they were found in his bedroom—yet admitted that law enforcement would likely find his DNA on the weapons. Specifically, Akhavan claimed that the guns belonged to his roommate, Keith McCarty, who was a co-founder of Eaze and a co-conspirator in the Scheme. Specifically, Akhavan claimed that his roommate would hide the firearms in Akhavan's room when McCarty had escorts over to party. Akhavan also denied that the crack belonged to him. Akhavan was arrested and detained on state charges for being a felon in possession of a firearm. (PSR ¶ 42).

III. The Presentence Report

The U.S. Probation Office determined that the total offense level for Count One is 43. The offense calculation for the defendant is as follows:

Base Offense Level: Pursuant to U.S.S.G. § 2B1.1(a)(1), the base offense level is seven. (PSR ¶ 47). Pursuant to U.S.S.G. § § 2B1.1(b)(1)(N), because the loss exceeded $150,000,000 but was less than $250,000,000, 26 levels are added. (PSR ¶ 48).

10 or more Victims: Pursuant to U.S.S.G. § 2B1.1(b)(2)(A)(i), two points are added because the offense involved ten or more victims. (PSR ¶ 49).

Conduct outside United States/Sophisticated Means: Pursuant to U.S.S.G. § 2B1.1(b)(10)(B) and 2B1.1(b)(10)(C), because a substantial part of a fraudulent scheme was committed from outside the United States, and the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means, two points are added. (PSR ¶ 50).

Gross Receipts In Excess of $1,000,000: Pursuant to U.S.S.G. § 2B1.1(b)(17)(A), because the defendant derived more than $1,000,000 in gross receipts from one or more financial institutions as a result of the offense, two points are added. (PSR ¶ 51).

Leader / Organizer Of a Criminal Activity with 5 or More Participants: Pursuant to U.S.S.G. § 3B1.1(a), a four-level increase is warranted because the defendant was an organizer or leader of a criminal activity that involved five or more participants or was otherwise extensive. (PSR ¶ 53).

The defendant is assigned to Criminal History Category I. (PSR ¶¶ 61, 63). Accordingly, the applicable Guidelines range is life imprisonment. (PSR ¶ 96). Probation recommends a sentence of 96 months' imprisonment. (PSR at 37).

Discussion

At the outset, the Government recognizes that the Guidelines range of life imprisonment, which is largely driven by the substantial loss amount, overstates the defendant's conduct. However, each of the relevant enhancements under the Guidelines appropriately capture distinct aspects of the defendant's criminal conduct, such as his role as a leader in a large criminal operation with many members; the large number of victims who were defrauded by the defendant; the sophistication of the defendant's scheme, as well as the deliberate use of jurisdictions outside of the United States in order to perpetrate the Scheme; and the large multi-million dollar profits that the defendant made as a result of his participation in the Scheme. In light of all of these factors, and as set forth in more detail below, a substantial term of imprisonment, below the Guidelines range of life, is warranted and necessary based on the sentencing factors the Court must consider under 18 U.S.C. § 3553(a).

Seriousness of the Offense and Need for Just Punishment

A substantial term of imprisonment, below the Guidelines range, is necessary to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense. 18 U.S.C. § 3553(a)(2)(A).

The defendant's criminal conduct in this case was serious: for a period of three years Akhavan was the leader of a highly sophisticated international fraud scheme. As shown at trial, the defendant planned and executed a scheme to deceive United States banks and other financial institutions, including Visa and MasterCard, into processing over one hundred and fifty million dollars in credit and debit card payments for the purchase and delivery of marijuana products. The defendant's Scheme was sophisticated and multi-layered. In particular, the defendants' Scheme involved the purchase and use of shell companies that were purchased for the sole purpose of facilitating the Scheme. The shell companies were used to open overseas bank accounts, which were in turn used to process the unlawful Eaze transactions. For each of the Phony Merchants, the defendants' Scheme also utilized fictitious webpages that were designed to hide the true nature of the transactions from banks and credit card companies. The defendants even created fake web traffic for those websites, to make the websites look legitimate.

Adding a further layer of obfuscation to the Scheme, Akhavan directed the members of the conspiracy to implement cookie technology in order to ensure that customers would not be confused by the descriptors appearing on their credit card statements, which could result in the customers contacting their issuing banks, who in turn would shut down the Scheme. As Akhavan explained to his co-conspirators, the use of "[t]he cookie tech[nology] on the descriptor urls [was] vital." (GX 302 at 62). The evidence at trial made it clear that Akhavan was responsible for

overseeing the implementation of this cookie technology. (*Id.* at 63 (John Wang asking Akhavan what Eaze needed to do for the cookie implementation); 5 (Darcy Cozzetto asking Akhavan who the Eaze team should talk to in order to get cookies implemented)).

Akhavan's role as the principal leader and architect of the Scheme is another factor that demonstrates the serious nature of his conduct.[1] The witnesses and exhibits from trial all demonstrate that Akhavan was the principle leader and mastermind behind the Scheme. (Tr. 176, 710, 726-727, 730-731, 1445, 1560, 1838-39, 2254; GX 411, 417, 4004, 4002). For example, during a meeting at Akhavan's office between Akhavan, Weigand, Oliver Hargreaves, and other co-conspirators that took place in January 2018, Akhavan drew a preliminary overview of a fraudulent processing model that would be used for the Eaze transactions on a white board. (Tr. 727). Among other things, the diagram included the use of phony merchants, which was a key part of the Scheme that was eventually implemented. Akhavan organized a subsequent meeting in March 2018 (the "March 2018 Meeting") in order to explain the Scheme to other co-conspirators, including employees at Eaze and the dispensaries. (Tr. 1553). During that meeting, Akhavan explained in detail how the Scheme would operate, including the use of fake merchants with overseas bank accounts, which Akhavan would arrange. (Tr. 1560). During both phases of the Scheme, Akhavan's co-conspirators reported to, and took direction from him with regard to the Scheme's operations.

During the course of the Scheme, Akhavan also resorted to threats and intimidation in order to keep the Scheme going. Specifically, in March 2018, Akhavan sent Jim Patterson, the CEO of Eaze at the time, a series of threatening phone messages. The messages stated, "see your processing with others while I pay for your merchants. Get ready to get fucked. You're in deep shit." (Tr. 1547). After receiving these messages, Patterson spoke with Akhavan on the phone. During that conversation, Akhavan again threatened and intimidated Patterson, stating in substance and in part, "You fucking piece of shit. You little worm. I've lost tons of money working with you. You go behind my back. You know, you better figure out some way to make sure that I get paid back." (Tr. 1548). Akhavan also demanded that he get paid a higher rate for processing the Eaze transactions. Patterson was aware that Akhavan had made threats to others in the past and interpreted Akhavan's messages to be a physical threat to him. (Tr. 1547-48). Akhavan's willingness to resort to threats of violence further demonstrates the seriousness of the offense conduct.

Although the defendant's Scheme did not result in Issuing Banks losing money on the Eaze transactions, the defendant's Scheme and others like it are enormously costly for banks and credit card companies. Other similar schemes include the unlawful processing of miscoded online gambling, prohibited pornography, and illegal pharmaceuticals. (*See*, *e.g.*, Tr. 1884). As a result of criminal activity like the defendant's, financial institutions must expend significant financial resources in order to protect the integrity of the global financial system by detecting and preventing criminal actors like the defendants from misusing bank accounts and credit card networks. For example, the head of fraud prevention for Citibank explained that the annual operating expenses for his group are $276 million, including $18 million in technology investments. (Tr. 2097). Such

[1] In terms of relative culpability, the Government views Akhavan, as the leader and mastermind of the Scheme, as the most culpable participant in the conspiracy.

significant expenditures are necessary as a result of schemes like the defendant's, which deceived financial institutions around the globe.

In sum, the totality of Akhavan's conduct during the Scheme was very serious and a substantial term of imprisonment, below the Guidelines, is necessary in order to reflect the seriousness of the offense, to promote respect for the law, and to provide just punishment for the offense.

Protecting the Public from Further Crimes of the Defendant

The defendant's actions during the course of the Scheme, as well as his actions since he was arrested, demonstrate that a substantial sentence, below the Guidelines range, is necessary in order to protect the public from further crimes of the defendant. 18 U.S.C. § 3553(a)(2)(C).

During the course of the Scheme, Akhavan's actions demonstrated that he believed he was above the law. For example, during the March 2018 Meeting, Akhavan bragged to Patterson that his bank was under investigation by the FBI, and that "every three-letter agency [was] after [Ahavan]." (Tr. 1159). In addition, during that same meeting, Akhavan told the attendees, in sum and substance, that the risk of criminal prosecution for him for his participation in the Scheme was very high ("eight, nine, or ten"). (Tr. 1839). Despite Akhavan's knowledge that he was under investigation by the FBI, and despite his understanding that he was exposed to an enormous risk of prosecution by participating in this criminal conspiracy, Akhavan continued to engage in the same criminal activity until the Scheme collapsed and he had no choice but to stop.

Akhavan's actions since his arrest also demonstrate that he views himself as completely above the law. As the Court is aware, Akhavan's list of violations of pretrial release are lengthy, ranging from using cocaine while in an inpatient drug treatment program, to far more serious violations including possessing firearms and attempting to tamper with an ongoing law enforcement investigation into his gun possession. (*See* Dkt. 150 at 4-5). Specifically, as described above, during an October 2020 incident in which Akhavan was questioned by the LAPD, Akhavan lied to the LAPD officer and told him that he was not on probation, even though he was then serving his term of probation in connection with his state convictions. The following month, while on probation in a California state case, and while on pretrial release in this case, Akhavan possessed two firearms, one of which was a loaded semi-automatic pistol, with a high-capacity magazine containing 12 rounds—and a prescription bottle that appeared to contain crack cocaine. When Akhavan was questioned about the guns by the LAPD, he made up a ridiculous story and falsely claimed that his roommate would hide the guns in Akhavan's room when his roommate had escorts over to party.

Akhavan's arrest after the gun incident did not deter him from continuing to commit crimes (while incarcerated). In telephone calls placed by Akhavan while he was detained in California, Akhavan talked to an unknown male ("UM") about steps that could be taken to get an individual, referred to as "Sal," to sign an affidavit representing that the guns found on November 5 did not belong to Akhavan. In a November 13 telephone call, Akhavan told UM that Akhavan "took [the guns] to give them to Sean," and that his DNA was on the guns because Akhavan was the one that hid them, but that UM should "tell Sal, and tell them, that they better write their affidavit or they're

fucking done." A few days later, on November 15, Akhavan reiterated to UM that "[i]f he doesn't [sign the affidavit], I'm going to fuck him so hard he's not going to know what do." When UM asked for "some ideas on how to fuck him," Akhavan responded that he would "think about some things for him," and added that Akhavan was "done protecting him." In short, Akhavan was actively attempting to tamper with at least one witness with information relevant to the firearms charges, and appeared to threaten potential physical harm to that witness if he did not comply with Akhavan's demands.

All of these actions demonstrate Akhavan's total disregard for the law. A substantial term of imprisonment, below the Guidelines range, is necessary to deter Akhavan from committing similar crimes in the future and to protect the public from future crimes of the defendant.

Adequate Deterrence to Other Sophisticated and Calculating Criminals

A substantial term of imprisonment is also necessary to adequately deter other sophisticated and calculating criminals like Akhavan from similar criminal conduct. 18 U.S.C. § 3553(a)(2)(B). General deterrence is that much more important in a case like this where the conduct was deliberate, sophisticated, planned in advance, and unfolded over a period of years. A substantial term of imprisonment is necessary to deter others from committing similar crimes by showing them that they risk a substantial term of imprisonment if they are caught.

In addition, the need to deter others is particularly strong here because the defendant's Scheme was extremely profitable. The defendant alone made in excess of €5,000,000 for the dirty payment processing services that he provided to Eaze. (GX 1518). In total, over a period of three years, Akhavan and his co-conspirators charged Eaze and the dispensaries more than approximately $17,000,000 in exchange for processing illegal transactions. Given the enormous financial incentives for criminals like Akhavan and his co-conspirators to engage in similar schemes, a substantial sentence is necessary in order to adequately deter others from doing so.

The need for adequate deterrence is even greater here given the difficulty in detecting sophisticated schemes like Akhavan's. Akhavan and his co-conspirators took numerous steps to ensure that they were not caught. For example, Akhavan insisted on using methods of communication, such as ProtonMail and Telegram, that were fully encrypted, located abroad, and had enhanced security features. (Tr. 1566, 746). As Patterson explained at trial, Akhavan expressed a preference for using services like Telegram because "[t]he messages weren't able to be read or intercepted by law enforcement." (Tr. 1567). With respect to ProtonMail, Oliver Hargreaves explained that it was highly encrypted and used "[f]or illegal activities." (Tr. 747). Akhavan also had a special phone with a different communication application that he used to engage in criminal activity. (Tr. 1567). That phone was even more secure than Telegram and the messages could not be read or intercepted by law enforcement. (*Id.*). The deliberate use of communication platforms such as these makes it far more difficult for law enforcement to detect and prosecute crimes such as Akhavan's. For example, law enforcement cannot execute search warrants on ProtonMail and Telegram, making it more difficult to obtain critical evidence.

Akhavan's scheme also used other techniques to avoid detection by law enforcement and to make prosecution more difficult. Among other things, Akhavan relied on overseas merchants

and bank accounts, none of which were in his own name. (*See*, *e.g.*, GX 3702). The use of overseas bank accounts and phony merchants made it more difficult to tie the scheme back to Akhavan. In addition, overseas bank accounts were used to make payments to Akhavan and his co-conspirators, making it far more difficult to trace the funds that were paid to them. These types of techniques can thwart law enforcement efforts to prosecute criminals like Akhavan, as well as efforts to forfeit criminal proceeds.

A substantial sentence, below the Guidelines Range, is therefore needed in order to deter others from pursuing similar schemes, which are planned in advance, highly lucrative, and difficult to detect by law enforcement officials.

History and Characteristics of the Defendant

The defendant's background provides no mitigation or excuse for his conduct. Akhavan reports having a difficult childhood. Specifically, he was raised in Iran by both parents and left Iran in 1984 as a political refugee. (PSR ¶ 68). Akhavan eventually came to the United States and attended college for period of time. Akhavan is a naturalized citizen. (PSR ¶ 75). Akhavan is married and has one daughter and one stepdaughter. Akhavan is currently in the process of going through a divorce. (PSR ¶ 73).

Akhavan reports several health issues. He suffers from extreme back pain as the result of a car accident in 2000. (PSR ¶ 78). He also has restless legs syndrome which causes him pain in his legs. (PSR ¶ 79). Akhavan also suffers from stomach problems as a result of taking medications that he was prescribed for his health problems. (PSR ¶ 80).

Akhavan has a history of substance abuse problems. He reports that he used cocaine on a daily basis from 2018 until his arrest in this case. (PSR ¶ 84). As the Court is aware, Akhavan participated in drug treatment programs while on release in this case. While in the first program in July 2020, he tested positive for cocaine and suboxone. As a result, he was discharged from the program. Akhavan entered another inpatient drug treatment program in September 2020 and again tested positive for cocaine while in the program.

Akhavan reports that he has operated his own company which "created software for billing" since 2006. (PSR ¶ 89). Akhavan's description of his business to Probation deviates from the evidence presented at trial. Hargreaves explained that Akhavan's business was "adult content," which he described as people paying subscriptions in order to view adult pornography. (Tr. 694). Akhavan also conducted the Scheme through the use of this same company, Quantum. (*See, e.g.*, Tr. 1297, 1301, 1375). Between 2016 through 2019, Akhavan reported earning enormous sums of money. Specifically, he reported earning the following gross income figures in those years: $5,501,459 (2016), $14,020,057 (2017), $5,057,323 (2018), and $1,432,590 (2019). (PSR ¶ 91).

The defendant has one prior conviction in 2019 to five counts of criminal threats and possession of an assault weapon. (PSR ¶ 61).

Taking into consideration the history and characteristics of the defendant, what emerges is a picture of a defendant who, despite a challenging childhood, managed to form a highly successful

and lucrative business. Nonetheless, despite enormous financial success, the defendant held himself above the law and pursued millions of dollars through a years-long fraud scheme. The fact that the defendant participated in this scheme despite his financial success is deeply troubling. It appears that he had other avenues to earn an honest living without breaking the law and yet chose to orchestrate a sophisticated and lengthy criminal conspiracy. He appears to have been motivated by nothing more than greed.

In sum, the defendant's history and characteristics indicate that a substantial term of imprisonment, below the Guidelines, is necessary and appropriate.

Conclusion

For the foregoing reasons, the Court should impose a substantial term of imprisonment, below the Guidelines range, in addition to forfeiture.

Respectfully submitted,

AUDREY STRAUSS
United States Attorney

By: s/
Nicholas Folly
Tara La Morte
Emily Deininger
Assistant United States Attorneys
(212) 637-1060

Cc: Defendant (by ECF)