

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA

CR. No.: 20-CR-0020-MRD

v.

TONY MERTILE and
JUNIOR MERTILE,
Defendants.

**GOVERNMENT’S COMBINED SENTENCING MEMORANDUM FOR
DEFENDANTS TONY MERTILE and JUNIOR MERTILE**

In accordance with the plea agreements, and for the reasons set forth herein, the Government asks the Court:

- *for Defendant Tony Mertile*, to impose a low-end Guideline sentence of imprisonment of 145 months¹ (comprised of 121 months for Count 2 (Conspiracy to Commit Wire Fraud), plus a consecutive 24 months for Count 9 (Aggravated Identity Theft));
- *for Defendant Junior Mertile*, to impose a low-end Guideline sentence of imprisonment of 87 months² (comprised of 63 months for Count 2 (Conspiracy to Commit Wire Fraud), plus a consecutive 24 months for Count 11 (Aggravated Identity Theft));

and for *each* Defendant, to enter an order of restitution for \$4,456,927.36; and grant the Motions for Preliminary Order of Forfeiture, of specified assets, and the Orders of Forfeiture (Money

¹ The Presentence Report for Defendant TONY MERTILE currently calculates the Guideline range as 121-151 months for Count 2 (Conspiracy to Commit Wire Fraud), plus the consecutive 24 months for Count 9 (Aggravated Identity Theft), *for a combined Guideline range of 145 – 175 months*. ECF 181, Presentence Report, ¶ 106. The Defendant made various objections, *see infra*, Section I, Objections. If the Defendant’s objections are sustained, and the Guideline range changes, the Government will amend its sentencing recommendation at the Sentencing Hearing, to make the agreed-upon low-end Guideline recommendation.

² The Presentence Report for Defendant JUNIOR MERTILE currently calculates the Guideline range as 63-78 months for Count 2 (Conspiracy to Commit Wire Fraud), plus the consecutive 24 months for Count 11 (Aggravated Identity Theft), *for a combined Guideline range of 87-102 months*. ECF 174, ¶ 118. The Defendant made various objections, *see infra*, Section I, Objections. If the Defendant’s objections are sustained, and the Guideline range changes, the Government will amend its sentencing recommendation at the Sentencing Hearing, to make the agreed-upon low-end Guideline recommendation.

Judgment) in the amount of \$1,214,294.75,³ as agreed to by the Defendants in their Plea Agreements.

As described herein, co-defendants TONY MERTILE and JUNIOR MERTILE, with their co-defendants and other co-conspirators, orchestrated a massive fraud scheme with co-defendants Allen Bien-Aime and James Legerme. Using fraudulently obtained identities and a network of fraudulently opened bank accounts in the names of others, TONY MERTILE, JUNIOR MERTILE, and their co-Defendants, filed thousands of fraudulent claims for government benefits, primarily for unemployment insurance relief offered to aid struggling Americans during the COVID-19 pandemic. Their criminal conduct was extensive, pervasive, and egregious. In total, TONY MERTILE, JUNIOR MERTILE, and their co-defendants stole *at least* \$4.8 million.

I. OUTSTANDING OBJECTIONS

Defendant TONY MERTILE filed a timely objection to the application of a +4 enhancement under U.S.S.G. § 3B1.1(a) (Aggravating Role Adjustment) and to the lack of a reduction under U.S.S.G. § 4C1.1, the Zero Point Offender Guideline. *See* ECF 163 (Def. Tony Mertile's Objection to PSI Report and ECF 181-3 (Addendum to Presentence Report (PSR))).

In addition, on March 7, 2025, both Defendants TONY MERTILE and JUNIOR MERTILE filed Notices of Notice Of Adoption Of Codefendant Allen Bien-Aime's Objection To PSI Report Regarding +2 Level 2B1.1(b)(11)(A) OR (B). *See* ECF 190 and 191.

³ As set forth in ECF 167 (TONY MERTILE) and 169 (JUNIOR MERTILE), in the *Government's Motions For (1) Preliminary Order Of Forfeiture And (2) Order Of Forfeiture (Money Judgment)*, in their respective Plea Agreements (ECF 135 (TONY MERTILE)); 136 (JUNIOR MERTILE), the Defendants agreed to forfeiture of specified assets and that an amount of \$4,857,191 constitutes proceeds of the conspiracy charged in Count 2, and that that each will forfeit a sum of money in the amount of \$1,214,294.75 in the form of a forfeiture money judgement.

Finally, in their respective Memorandum In Aid Of Sentencing And Incorporated Motion For Downward Variance (Sentencing Memorandum) (ECF 179 (TONY MERTILE); ECF 180 (JUNIOR MERTILE)), contrary to well-established law and agreements within their plea agreements, the Defendants appear to make two other untimely objections, first as to the Sophisticated Means enhancement under U.S.S.G. § 2B1.1(b)(10), and second, as to the Defendants' being responsible for the negotiated and agreed-upon loss amount. *See* Sentencing Memoranda, ECF 179 (TONY MERTILE), ¶ 34, 33, 43; ECF 180 (JUNIOR MERTILE), ¶ 32, 31.

The Government now responds to these various Objections.

A. Applicable Law Governing Burden of Proof for Objections to Guideline Calculations

In considering objections and determining what guideline adjustments apply, the Court must find that the Government has made a showing of any fact necessary and relevant to sentencing by a preponderance of the evidence. *United States v. Flete-Garcia*, 925 F.3d 17, 28 (1st Cir. 2019). The Court has “considerable discretion” in determining what evidence should be regarded as reliable for such fact-finding. *Id.* at 28. Because at the sentencing phase a defendant has no right to confront witnesses against him and sentencing courts may rely on hearsay evidence, *see United States v. Rodriguez*, 336 F.3d 67, 71 (1st Cir. 2003), the Court may appropriately rely on documentary information such as the PSR, affidavits, exhibits, and submissions of counsel. *United States v. Curran*, 525 F.3d 74, 78 (1st Cir. 2008) (quoting *United States v. Ranney*, 298 F.3d 74, 81 (1st Cir.2002)). The Court may “evaluate virtually *any* dependable information” to determine the probative value of such information with respect to issues material to sentencing. *United States v. Bradley*, 917 F.2d 601, 605 (1st Cir. 1990) (emphasis added); *see, e.g., United States v. Acevedo-Lopez*, 873 F.3d 330, 340 (1st Cir. 2017) (relying upon hearsay proffer of the AUSA).

The Court may consider relevant information without regard to its admissibility under the rules of evidence applicable at trial, provided that the information has sufficient indicia of reliability, U.S.S.G. § 6A1.3(a), including out-of-court statements by witnesses. *United States v. Lee*, 892 F.3d 488, 492 (1st Cir. 2018). Such indicia may include details, internal consistence, and corroboration by multiple witnesses. *United States v. Green*, 426 F.3d 64, 67 (1st Cir. 2005) (emphasis added).

Evaluation of the submitted information need not involve a hearing. Rather, “[a]t sentencing, evidentiary hearings are the exception, not the rule.” *Flete-Garcia*, 925 F.3d at 34 (citing *United States v. Shattuck*, 961 F.2d 1012, 1014-15 (1st Cir. 1992)). The parties need only have an “adequate opportunity to present information to the court” about any sentencing factor that is “reasonably in dispute.” *Id.* at 35; U.S.S.G. § 6A1.3(a). Where the Government provides documentary support sufficient for factual findings, there is no need to “bolster” the evidence by calling a live witness. *See United States v. Gerante*, 891 F.2d 364, 367 (1st Cir. 1989).

B. Objection to +2 Under U.S.S.G. § 3B1.1(a) (TONY MERTILE)⁴

Defendant TONY MERTILE has objected to the +4 adjustment for his role in the offense under U.S.S.G. § 3B1.1(a) at ¶ 61 of the PSR. *See* ECF 181-1 and ECF 163, Objection to PSI.

U.S.S.G. § 3B1.1 established a tiered approach for aggravating role enhancements. For criminal activity that involved 5 or more participants, or “was otherwise extensive,” a +4 enhancement applies for a defendant who was an organizer or leader, and a +3 enhancement applies for a defendant who was a manager or supervisor. U.S.S.G. § 3B1.1(a) and (b), & Application Note 2. For a defendant involved in other criminal activity that did not involve 5 or more participants or that was not “otherwise extensive,” and who was an organizer, leader,

⁴ The Government incorporates the Response by the Probation Officer to TONY MERTILE’s U.S.S.G. 3B1.1(a) Objection in the PSR, ECF 181-3, as if set forth fully herein.

manager, or supervisor” of one or more participant, a +2 enhancement applies. U.S.S.G. § 3B1.1(c), & Application Note 2.

For a U.S.S.G. § 3B1.1(a) and (b) role adjustment to apply, the Government must show *first*, the scope of the criminal activity, specifically that it involved 5 or more participants, or was otherwise extensive, and *second*, a defendant’s status in the criminal activity. *See United States v. Figaro-Benjamin*, 100 F.4th 294, 306-08 (1st Cir. 2024); *United States v. Coplin-Benjamin*, 79 F.4th 36 (1st Cir. 2023).

To assess the numerosity aspect of the scope of criminal activity, the Guidelines provide that a “participant” is a person who is criminally responsible for the commission of the offense, but need not have been convicted.” U.S.S.G. § 3B1.1, Application Note 1).

To be considered a participant, it is only necessary that an individual gives knowing aid in some aspect of the criminal activity. Similarly, an individual can be considered a participant when his or her acts “give rise to an inference of complicity sufficient to ground a finding that [the individual] was a participant in the criminal activities.”

United States v. Acevedo-López, 873 F.3d 330, 336-37 (2017) (affirming § 3B1.1(a) enhancement). *See also United States v. Tavares*, 705 F.3d 4, 30 (2013) (holding that an immunized witness who was part of the criminal activity may be a “participant”). Further,

[w]ho is considered a member of the conspiracy for purposes of the numerosity criterion is to be broadly construed, and all persons involved in the conspiracy—including outsiders—can be counted towards considering the conspiracy “extensive.” *See id.* (quoting USSG § 3B1.1 cmt. 3). Courts may look beyond the number of participants to evaluate whether a conspiracy was “extensive” by considering “the totality of the circumstances, including ... the width, breadth, scope, complexity, and duration of the scheme.”

United States v. Goodwin, 617 Fed. Appx. 12, 15 (1st Cir. 2015).

For a U.S.S.G. § 3B1.1(a) role adjustment, a defendant must act as either a leader or an organizer.

A defendant acts as a leader where he “exercise[s] ... some degree or dominance of power in a hierarchy” and has “authority to ensure other persons will heed commands,” and he “may be classified as an organizer, though perhaps not as a leader, if he coordinates others so as to facilitate the commission of criminal activity.”

United States v. Aguasvivas–Castillo, 668 F.3d 7, 15 (1st Cir.2012). *See also United States v. Poliero*, 81 F.4th 96, 100-01 (2023) (rejecting defendant’s claim that he was not a leader / organizer and that at most, a manager / supervisor enhancement applied) (citations omitted); *United States v. Jimenez*, 946 F.3d 8, 14-15 (1st Cir. 2019) (affirming the +4 U.S.S.G. § 3B1.1(a) leadership enhancement; finding ample evidence that the defendant recruited key players, was the common actor in fraudulent activity, and received the largest share of the fraud proceeds). “[A] defendant needs only to have led or organized one criminal participant, besides himself of course, to qualify as a leader or organizer under § 3B1.1(a).” *United States v. Appolon*, 695 F.3d 44, 70 (1st Cir. 2012); *United States v. Coplin-Benjamin*, 79 F.4th at 41.

Furthermore, a conspiracy may have more than one leader. *See United States v. Coplin-Benjamin*, 79 F.4th at 42; *United States v. Rodriguez-Reyes*, 714 F.3d 1, 13 (2013) (affirming application of the leadership enhancement). “The relevant inquiry is only whether [defendant] was *a leader of the conspiracy*, not whether he was the leader. There can be more than one leader of a conspiracy.” *See United States v. Rodriguez-Reyes*, 714 F.3d 1, 13-14 (2013) (emphasis added) (affirming the +4 U.S.S.G. § 3B1.1(a) leadership enhancement).

Application Note 4 of U.S.S.G. 3B1.1 states that:

In making the determination of whether someone is an “organizer or leader” or merely a “manager or supervisor,” courts should consider “the exercise of decision making authority, the nature of participation in the commission of the offense, the recruitment of accomplices, the claimed right to a larger share of the fruits of the crime, the degree of participation in planning or organizing the offense, the nature and scope of the illegal activity, and the degree of control and authority exercised over others.”

However, the First Circuit has cautioned that the list of factors in Application Note 4 “is representative rather than exhaustive, and proof of each and every factor is not necessary to establish that a defendant acted as an organizer or leader.” See *United States v. Coplin-Benjamin*, 79 F.4th at 41 (citations omitted).

With any of the U.S.S.G. § 3B1.1 aggravating role adjustments, a formal, hierarchy or chain of command is not required. *United States v. Figaro-Benjamin*, 100 F.4th at 306-08. Further, multiple persons can serve leadership roles. “[T]he existence of another leader -- even one superior to [defendant] in the scheme’s hierarchy -- does not foreclose the possibility of [defendant] also acting as a leader.” *United States v. Coplin-Benjamin*, 79 F.4th at 42.

The First Circuit has held that it is “a relatively low bar” to show that a defendant exercised some control over another criminal actor. *United States v. Figaro-Benjamin*, 100 F.4th at 307. In fact, the supervisory authority may be minimal and may have been exercised on a single occasion for a § 3B1.1 enhancement to apply. *Id.* at 307 (finding that defendant’s “role involved at least a minimal degree of control over others, on at least one occasion; defendant’s text messages that showed that he sent a taxi to transport two participants to assist with criminal activity, as well as text messages in which he advised other participants of a date for activity and questioning when another participant didn’t respond promptly.) If a defendant takes a role in recruiting at least one person to aid in the conspiracy, that can be sufficient for the a managerial-role enhancement. See *United States v. Savarese*, 686 F.3d at 19-20 (affirming application of U.S.S.G. 3B1.1(c) enhancement). In *Savarese*, the Court rejected the defendant’s claim that the enhancement didn’t apply because he didn’t hold any supervisory role, and found that his role in recruiting another was sufficient.

That “[Defendant] was by no means the mastermind of the operation, that is not the standard by which “managerial” status is governed. A defendant’s exhibitions of

authority need be neither supreme nor continuous; we have even held that, in some circumstances, the government need only show by a preponderance of the evidence “that the defendant exercised authority or control over another participant on one occasion.”

Id. at 20 (citation omitted). See also *United States v. Prange*, 771 F.3d at 35 (affirming application of U.S.S.G. 3B1.1(c) enhancement, finding that “at a minimum, [defendant] recruited Jordan and multiple other executives into this scheme by introducing them to E.H., gauging their willingness to issue kickbacks, and recommending them to the agent.”)

First, as to the number of individuals involved in the criminal activity, in addition to the 4 defendants charged in this case, the evidence shows that criminal activity involved multiple other participants, and certainly more than 5 participants that the U.S.S.G. § 3B1.1(a) enhancement requires. Counting each of the 4 charged Defendants, the following 5 participants (T.M., S.A., M.A., P.C., S.S.)⁵ who texted with TONY MERTILE as shown by the Exhibits 24-28 (described below), and Luckson Louissant,⁶ at a minimum, the criminal activity involved 10 participants.

⁵ Because none of these individuals have been charged, they have been identified by initials in this filing. Text messages between TONY MERTILE and each of these participants have been filed (under seal) as Exhibits 24-28 to this Memorandum. Each Exhibit identifies the full name of the participant.

⁶ As set forth at pp. 6-7, and Exhibits 1 and 2, to ECF 187, Government’s Sentencing Memorandum (Defendant James Legerme), which is incorporated herein by reference, co-defendant Legerme recruited his cousin, Luckson Louissant, to aid him and his co-conspirators. Louissant created email addresses for his co-conspirators. Text messages between Legerme and Louissant show communications relating to Louissant’s efforts for Legerme, as well as for “T” [Tony MERTILE]; “P” [Junior “Peanut” MERTILE]; “G,” “Fat Ass,” [uncharged co-conspirator P.C.]. For example, in one text exchange, Legerme and Louissant stated:

-Legerme: 2:59 PM - Still have 20 left but I’m giving it to t but I need lol (Emoji)
-LOUISSAINT: 2:59 PM - ok 100 more
-LOUISSAINT: 3:00 PM - ?
-Legerme: Yes go ahead, I owe you 200, P owe 100, Fat 100, T 100 right now.

In the text exchange, Legerme was telling LOUISSAINT that he still had email addresses and passwords to be used, but that he was giving those email addresses/passwords to “t,” who refers to TONY MERTILE, and further explained that he, and his co-conspirators, including “T” [TONY MERTILE] owed Louissant \$100 for his work.

s

The facts set forth in Section IIA (Nature and Circumstances of the Offense (18 U.S.C. § 3553(a)(1))), in ECF 181, the Presentence Report for TONY MERTILE, and summarized below, show, well beyond a preponderance that TONY MERTILE was a leader and/or organizer of the criminal activity to which he has pled guilty.

- As shown in Exhibits 24 - 28, TONY MERTILE recruited, directed, and coordinated with T.M., S.A., M.A., P.C., S.S. to further the goals of the conspiracy.
 - Exhibit 24 includes excerpts of text messages between Tony MERTILE (using cell phone number 3678) and T.M. (referred to in TONY MERTILE's messages as "Mara").
 - Exhibit 25 includes excerpts of text messages between Tony MERTILE (using cell phone number 3678) and S.A. (referred to in TONY MERTILE's messages as "Blac Girl").
 - Exhibit 26 includes excerpts of text messages between Tony MERTILE (using cell phone number 3678) and M.U. (referred to in TONY MERTILE's messages as "Tika").
 - Exhibit 27 includes excerpts of text messages between Tony MERTILE (using cell phone number 3678) and P.C. (referred to in TONY MERTILE's messages as "Fat Ass").
 - Exhibit 28 includes excerpts of text messages between Tony MERTILE (using cell phone number 3678) and S.S. (referred to in TONY MERTILE's messages as "Money").
- Tony MERTILE's text messages and phone communications show that he was in contact⁷ with each of the co-defendants and communicated with them each about the fraud, whereas the evidence does not show that the others communicated to the same extent with each other about the fraud scheme.⁸

⁷ A "contact" can be a call, a text, or a voice mail. Contacts only reflect activity on a cell service network, not wi-fi enabled communications.

⁸ To show the frequency of contacts between TONY MERTILE and the other co-defendants, the Government provides that following data. According to toll records and pen register data, Bien-Aime and TONY MERTILE were in regular contact from at least April 2020 through August 2020. Bien-Aime appears, according to toll data, to only be in contact with TONY MERTILE. TONY MERTILE, JUNIOR MERTILE, and James Legerme were all in contact with each other. TONY MERTILE (with one of his phones, referred to here as Target Telephone 1) and Bien-Aime (Target Telephone 2) had 137 contacts between April 14, 2020 and July 4, 2020. From July 4, 2020 through August 15, 2020, TONY MERTILE

- The largest volume of evidence and cash was seized from TONY MERTILE's residence, along with a currency counting machine.
- Cell site location information for the locations identified as banks and withdrawals show that Tony MERTILE was in the area of these banks and ATMs more than the other co-defendants.

C. Objection as to Zero Point Offender (TONY MERTILE)

Defendant TONY MERTILE also objects to lack of a 2 point reduction under U.S.S.G. § 4C1.1, the Zero Point Offender provision. In relevant part, U.S.S.G. § 4C1.1 provides that:

If the defendant meets all of the following criteria:

- (1) the defendant did not receive any criminal history points from Chapter Four, Part A;
- (10) the defendant did not receive an adjustment under §3B1.1 (Aggravating Role); and

decrease the offense level determined under Chapters Two and Three by 2 levels.

U.S.S.G. § 4C1.1. The Defendant's role in the conspiracy, and consequent role adjustment under U.S.S.G. § 3B1.1(a), makes him ineligible for a reduction under U.S.S.G. § 4C1.1.

D. Objection as to +2 Under U.S.S.G. § 2B1.1(b)(11)(A) or (B) – Possession and Use of an Authentication Feature (TONY MERTILE and JUNIOR MERTILE)

The Probation Department has found that a +2 enhancement applies under U.S.S.G. § 2B1.1(b)(11)(A). *See* ECF 181, ¶ 59 (PSR (TONY MERTILE), ECF 174, ¶ 60. Each of the Defendants has adopted the argument submitted by co-defendant Allen Bien-Aime. The enhancement is properly included in the Guideline calculation for Defendants TONY MERTILE and JUNIOR MERTILE, as well as the other co-defendants, for the reasons set forth Section IIA

(Target Telephone 1) and 9262 (BIEN-AIME's other phone), had 50 contacts. TONY MERTILE and JUNIOR MERTILE had 117 contacts between April 6, 2020 and September 29, 2020. TONY MERTILE and Legerme had 570 contacts between April 1, 2020 and October 1, 2020. JUNIOR MERTILE and Legerme had 283 contacts between August 21, 2020 and October 1, 2020 (tolls and pen register).

(Nature and Circumstances of the Offense (18 U.S.C. § 3553(a)(1))), those provided by the Probation Department in Response to the Objection by Defendant Bien-Aime,⁹ and those that will be addressed by the Government at the Sentencing Hearing in Response to arguments raised by counsel for Defendant Bien-Aime in his Sentencing Memorandum.

First,

[t]he term “authentication feature” means any hologram, watermark, certification, symbol, code, image, *sequence of numbers* or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified.

18 U.S.C. § 1028(d).

As described in greater detail below in Section II (During the course of their fraudulent endeavors, the co-defendants, including TONY MERTILE and JUNIOR MERTILE, had fraudulent funds deposited into fraudulently opened accounts for which they obtained debit cards. To withdraw the fraudulent proceeds, the co-defendants, TONY MERTILE and JUNIOR MERTILE, used PIN numbers for the debit cards to withdraw funds. The PIN number, as well as any other security features on the debit cards, constitute an authentication feature.

Next, the language of the Guidelines show that Defendants’ double-counting argument also fails. U.S.S.G. § 2B1.1(b)(11) states that an enhancement applies if the offense involved:

(A) the possession or use of any (i) device-making equipment, or (ii) authentication feature;

(B) the production or trafficking of any (i) unauthorized access device or counterfeit access device, or (ii) authentication feature; or

(C) (i) the unauthorized *transfer or use of any means of identification* unlawfully to produce or obtain any other means of identification, or (ii) the *possession of 5 or*

⁹ The Government also incorporates the Response to the Bien-Aime Objection by the Probation Officer in ECF 172-2, as if set forth fully herein.

more means of identification that unlawfully were produced from, or obtained by the use of, another means of identification,

U.S.S.G. § 2B1.1(b)(11) (emphasis added). Recognizing the potential for impermissible double counting, U.S.S.G. §2B1.6, the Guideline for the 18 U.S.C. § 1028A offense, prohibits application of specific offense conduct enhancement for “the transfer, possession, or use of a means of identification.”

If a sentence under this guideline is imposed in conjunction with a sentence for an underlying offense, do not apply any specific offense characteristic for the *transfer, possession, or use of a means of identification* when determining the sentence for the underlying offense.

U.S.S.G. § 2B1.6 (emphasis added). By its terms, that prohibition is specifically limited to specific offense conduct involving the “*transfer, possession, or use of a means of identification*,” which, for U.S.S.G. § 2B1.1(b)(11), would only include subpart (C) of that Guideline. *See United States v. James*, 744 Fed. Appx. 664, 666 (11th Cir. 2018) (“Section 2B1.6 does not bar all sentencing enhancement for defendants who are convicted under § 1028A, because not all § 1028A conduct involves only the transfer, possession, or use of another person’s means of identification.”). The First Circuit has held that U.S.S.G. § 2B1.6 does not prohibit application of an enhancement under U.S.S.G. § 2B1.1(b)(11), provided the enhancement is not based on conduct described in subpart (C) or the “trafficking” conduct in subpart (B) of U.S.S.G. § 2B1.1(b)(11), neither of which is the basis for the enhancement in this case. *See United States v. Jones*, 551 F.3d 19, 25-26 (1st Cir. 2008) (applying +2 enhancement for production of a fraudulent license under U.S.S.G. § 2B1.1(b)(10)(B) (prior version of U.S.S.G. § 2B1.1(b)(11)(B)), and finding that trafficking of means of identification was a “transfer” of a means of identification); *United States v. Sharapka*, 526 F.3d 58, 61-62 (1st Cir. 2008) (applying +2 enhancement for use of device making equipment under U.S.S.G. § 2B1.1(b)(10)(A) (prior version of U.S.S.G. § 2B1.1(b)(11)(A))). Other Circuits

have reached the same conclusion. *See United States v. Pendergrass*, No. 22-13018, 2025 WL 78172, at *9-10 (11th Cir. January 13, 2025) (recognizing that application of § 2B1.1(b)(11)(A), for use of an authentication feature, was proper, and did not constitute double-counting); *United States v. A.M.*, 927 F.3d 718, 720-21 (3rd Cir. 2019) (affirming application of +2 enhancement under subpart (A) of U.S.S.G. § 2B1.1(b)(11), which was found to be distinct from the conduct in subpart (C) of § 2B1.1(b)(11), for which the enhancement would be precluded under U.S.S.G. § 2B1.6); *United States v. Damyanov*, 503 Fed. Appx. 224, 225-26 (4th Cir. 2013) (“§ 2B1.6 does not exclude all conduct described in” U.S.S.G. § 2B1.1(b)(11);” affirming +2 enhancement under 2B1.1(b)(11)(B) based on production).

In this case, the Government agrees with the Probation Officer that the enhancement applies under U.S.S.G. § 2B1.1(b)(11)(A) (“the possession or use of any . . . (ii) authentication feature”). As described in the Probation Officer’s response, the Defendants and their co-conspirators’ conduct involved a much broader range of conduct than the conduct for which application of this enhancement would be prohibit under U.S.S.G. § 2B1.6. Moreover, the Defendants and their co-defendants possessed and used the authentication features for the debit cards which they used to withdraw fraudulent funds from the fraudulent bank accounts.

In summary, during the course of the conspiracy, each of the co-defendants, including TONY MERTILE and JUNIOR MERTILE, had fraudulent funds deposited into fraudulently opened accounts for which they obtained debit cards. To withdraw the fraudulent proceeds, the co-defendants, including BIEN-AIME, used PIN numbers for the debit cards to withdraw funds. The PIN number, as well as any other security features on the debit cards, constitute an authentication feature.

E. Objection / Challenge to Sophisticated Means Enhancement Under U.S.S.G. § 2B1.1(b)(10) (TONY MERTILE and JUNIOR MERTILE)

In their respective Sentencing Memoranda, the Defendants claim that “[t]he sophisticated means enhancement of +2 levels is also an artificial increase built into USSG 2B1.1 as in any computer and internet-based wire fraud prosecution the essential elements of USSG 2B2.2(b)(10)(C) are present and necessary for the completion of the charge.” *See* Sentencing Memos (ECF 179 (TONY MERTILE), ¶ 34); ECF 180 (JUNIOR MERTILE), ¶ 32). Although unclear if the Defendants are making an actual objection to the +2 Sophisticated Means enhancement under U.S.S.G. § 2B1.1(b)(10) or are simply attempting to minimize the scope of their massive fraud and aggravated identity theft conspiracy, the Court should overrule (if an objection is being made) or outright reject any suggestion that the Defendants’ and that the enhancement artificially inflates the Guideline range.

Under U.S.S.G. § 2B1.1(b)(10), the sophisticated means enhancement can apply if any of the following three circumstances are present:

- (A) the defendant relocated, or participated in relocating, a fraudulent scheme to another jurisdiction to evade law enforcement or regulatory officials;
 - (B) a substantial part of a fraudulent scheme was committed from outside the United States; *or*
 - (C) the offense otherwise involved sophisticated means and the defendant intentionally engaged in or caused the conduct constituting sophisticated means.
- ..

U.S.S.G. § 2B1.1(b)(10). In this case, for the reasons set forth in this Memorandum and in the PSRs,¹⁰ the +2 enhancement appropriately captures the scope and nature of this fraud and is warranted under U.S.S.G. § 2B1.1(b)(10)(C) [Offense Involved Sophisticated Means].

¹⁰ The Government incorporates the basis for the enhancement in the PSRs, as if set forth fully herein in. *See* PSRs, ECF 181 (TONY MERTILE)¶ 58 and ECF 174 (JUNIOR MERTILE), p. 15 (between ¶¶ 59 and 60)).

In finding that offense conduct involved “sophisticated means,” courts have regularly focused on the whether the conduct was intended to conceal the offense conduct and/or conceal proceeds and whether the conduct was repetitive and coordinated. *See United States v. Jimenez*, 946 F.3d 8, 15 (1st Cir. 2019) (“[s]ophisticated means are ‘especially complex or especially intricate offense conduct pertaining to the execution or concealment of an offense.’ The conduct must involve some greater level of concealment than a typical fraud of its kind.”) (citing *Pacheco-Martinez*, 791 F.3d 171, 179 (1st Cir. 2015)); *United States v. Nygren*, No. 1:16-cr-00106-JAW, 2018 WL 1733980, at *8 (D. Me. April 10, 2018) (“Taken together, although not each of these means would be extraordinarily sophisticated, the cumulative effect would have been to ‘facilitate [tax evasion] and to help conceal his [income and assets].’” (citing and quoting *United States v. George*, 841 F.3d 55, 61 (1st Cir. 2016). *See also United States v. Presendieu*, 880 F.3d 1228, 1244 (11th Cir. 2018). (“[R]epetitive, coordinated conduct designed to allow [a defendant] to execute his fraud and evade detection” may qualify as sophisticated.”); *United States v. Meadows*, 866 F.3d at 913, 917 (8th Cir. 2017) (quotations and citations omitted) (“Repetitive and coordinated conduct, though no one step is particularly complicated, can be a sophisticated scheme. . . .Overall, the sophistication of the offense conduct is associated with the means of repetition, the coordination required to carry out the repeated conduct, and the number of repetitions or length of time over which the scheme took place.”).

Although U.S.S.G. § 2B1.1, Application Note 9(B) provides examples of what may constitute “sophisticated means,” the First Circuit has repeatedly held that a scheme may viewed as “sophisticated” for application of U.S.S.G. § 2B1.1(b)(10), even if the manner in which the scheme was executed is not included in the examples in the commentary.

The list in the commentary of conduct that warrants the enhancement is not exhaustive. The defendant need not have done any of the things listed in order to qualify for the enhancement, so long as the offense as a whole shows a greater level of planning or concealment' than a typical fraud of its kind.

United States v. Pacheco-Martinez, 791 F.3d 171, 178-179 (1st Cir. 2015) (citation and quotation omitted). *See United States v. Foley*, 783 F.3d 7, 25-26 (1st Cir. 2015) (“The enumerated examples are by no means exhaustive, and as other circuits have recognized, “the enhancement properly applies to conduct less sophisticated” than the examples.”) (citation omitted).¹¹

As set forth in the PSRs, as summarized in Section IIA (Nature and Circumstances of the Offense (18 U.S.C. § 3553(a)(1))), and in this section, the Defendants’ and their co-Defendants’ conduct was extensive, repetitive, well-coordinated, and was designed to conceal the offense conduct. In summary, beginning on a date not later than January 2019, the Defendants began amassing an enormous library of fraudulently obtained identities and began a coordinated and concealed effort to defraud Government programs. They opened hundreds of bank accounts and obtained at least 943 debit cards, all in the names of other persons, primarily identity theft victims. They repeatedly applied for benefits from multiple government programs in the names of hundreds of identity theft victims, had fraudulently obtained funds deposited into the network of accounts, and then worked together to withdraw the funds in cash shortly after they were deposited. This massive fraud scheme relied upon and was orchestrated using multiple layers of deception, all

¹¹ Other Circuits have similarly held that conduct not referenced in the Guideline Commentary can support application of the U.S.S.G § 2B1.1(b)(1)(10) enhancement. *See United States v. Milligan*, 77 4th 1008, 1013-1014 (D.D.C. 2023) (finding that the commentary provides examples but that “several of our sister circuits agree that the enhancement can apply to conduct less sophisticated than the list articulated in the application note. After all, the examples are by their own terms simply illustrative, not exclusive.”); *United States v. Lopez*, 734 Fed. Appx. 674 (11th Cir. 2018) (“the illustrations in the application note are non-exclusive”); *United States v. Jennings*, 711 F.3d 1144, 1147 (9th Cir. 2013) (holding that “the list contained in the application note is not exhaustive. We agree with other circuits that the enhancement properly applies to conduct less sophisticated than the list articulated in the application note.”) (collecting cases).

intended to conceal not only the perpetrators of the fraud, but also the disposition of victim funds, thereby concealing the ultimate disposition of the funds. The nature and extent of the fraudulent acts undertaken, and the duration of time over which the Defendants and their co-conspirators successfully concealed their involvement in the fraud supports the enhancement. The planning and concealment involved in this scheme far surpassed that required for what may be viewed as “simple” fraud, which can be committed by means of an isolated instance of fraud or deceit. In addition, the Defendants’ recruited and worked together, and with others, to develop and execute a fraud scheme that was premised on multiple layers of deception and coordination to conceal and prolong the fraud.

Courts in the First Circuit have found similar, and even lesser efforts, to conceal and coordinate fraud schemes than those undertaken by the Defendants supported application of U.S.S.G § 2B1.1(b)(1)(10).¹² See *United States v. Kitts*, 27 F.4th 777, 781, 789-90 (1st Cir. 2022) (investment advisor misappropriated funds from three clients, and attempted to conceal her embezzlement, by creating a fake company, fake tax forms, and altered accounting statements); *United States v. George*, 841 F.3d 55, 66 (1st Cir. 2016) (defendant diverted funds from a transit authority, and used a shell corporation “to facilitate and to help to conceal his perfidy”). See *United States v. Jimenez*, 946 F.3d 8, 15 (1st Cir. 2019) (in a mortgage fraud scheme, defendant recruited

¹² Similar to the First Court, other Circuits have found that the enhancement applied in fraud and money laundering schemes that were equally or less involved and intricate than the conduct perpetrated by the Defendant. See *United States v. Meadows*, 866 F.3d 913 (8th Cir. 2017) (applying the enhancement in long term scheme that involved 69 victims to whom the defendant repeatedly lied to perpetrate the fraud and conducting lulling payments to conceal the fraud); *United States v. Aderinoye*, 33 F.4th 751, 755 (5th Cir. 2022) (finding sophisticated means enhancement applied; defendant’s actions, creating 40+ fraudulent bank accounts in the names of real and fictitious persons and business entities and transferring funds between the accounts, made it more difficult to detect the fraud); *United States v. Okeke*, 779 Fed. Appx. 389, 391-93 (7th Cir. 2019) (applying the enhancement in fraud and money laundering involving romance fraud and other fraud, in which defendant engaged in financial transactions below \$10,000 to avoid the bank’s reporting thresholds and would transfer money to a co-conspirator’s account).

straw buyers, and advised mortgagors as to making mortgage payments); *United States v. Foley*, 783 F.3d at 25 (in a mortgage fraud scheme, defendant used false disbursement authorization forms, false checks, and creating false deposit entries in bank accounts); *United States v. Evano*, 553 F.3d 109, 111-13 (1st Cir. 2009) (defendant and his wife engaged in a fraud scheme in which they ingested glass and thereafter claimed the glass was from food at hotels and restaurants, and submitted fraudulent insurance claims using false names and identifiers; finding that the defendant's use of false names, fake identification, and submission of fraudulent insurance claims "was enough to make their scheme more effective and difficult to thwart, and it is enough to justify the enhancement).

F. Objection / Challenge to the Loss Amount (U.S.S.G. § § 1B1.3 and 2B1.1(b)(1)) (TONY MERTILE and JUNIOR MERTILE)

Defendants' next objection disregards not only the agreement that they made in their respective plea agreement, but the plain language of the Guidelines and well-established case law regarding loss calculation for members of a conspiracy. In their Plea Agreements, each Defendant agreed that:

Beginning on an unknown date but not later than in or about January 2019 and continuing through on or about October 13, 2020 . . . [TONY MERTILE /JUNIOR MERTILE], *on his own, and in concert with unknown and known persons, including Allen Bien-Aime, [Junior Mertile/Tony Mertile], and James Legerme*, agreed to and did engage in a scheme to defraud and to obtain money by means of materially false and fraudulent pretenses, representations, and promises, for benefits and payments made available from federal and state government agencies.

Plea Agreements, ¶ 4a (emphasis added). Despite their agreement to the loss amount, the Defendants now challenge the agreed-upon loss amount. Each Defendant now claims that the loss amount is artificially high and that his actions are but a small part of the case, that are not accurately reflected in the resulting Guideline calculation due to each being held responsible for the full conspiracy loss. (ECF 179 (TONY MERTILE), ¶¶ 33, 43); ECF 180 (JUNIOR MERTILE), ¶ 31.

U.S.S.G. § 2B1.1 defines “loss” as “the greater of actual loss or intended loss.” U.S.S.G. § 2B1.1, Note to Table (A). “Actual loss” is defined as “the reasonably foreseeable pecuniary harm that resulted from the offense.” *Id.*, at Note to Table. “Intended loss,” by contrast, is defined as “the pecuniary harm that the defendant purposely sought to inflict [which] includes intended pecuniary harm that would have been impossible or unlikely to occur.” *Id.*, at Note to Table (C)(iii). “Since intended loss normally subsumes actual loss, intended loss is often the greater of the two.” *United States v. Flete-Garcia*, 925 F.3d at 28. The Guidelines further explain that

in the case of a jointly undertaken criminal activity (a criminal plan, scheme, endeavor, or enterprise undertaken by the defendant in concert with others, whether or not charged as a conspiracy), all acts and omissions of others that were—

- (i) within the scope of the jointly undertaken criminal activity,
- (ii) in furtherance of that criminal activity, and
- (iii) reasonably foreseeable in connection with that criminal activity;

that occurred during the commission of the offense of conviction, in preparation for that offense, or in the course of attempting to avoid detection or responsibility for that offense.

U.S.S.G. § 1B1.3(a)(1)(B). The First Circuit has recognized that for conspiracies, loss is determined not only by loss occasioned by an individual, but also by those reasonably foreseeable acts undertaken by his co-conspirators.

Section 2B1.1(b)(1) calls for a sentencing court to increase an offender’s offense level in theft and fraud cases according to the amount of loss resulting from the offense. A defendant in a jointly undertaken criminal activity is liable for the loss resulting from acts directly attributable to him and for the loss resulting from the reasonably foreseeable acts of others taken in furtherance of the jointly undertaken criminal activity. See U.S.S.G. § 1B1.3(a)(1), (3).

United States v. Codarcea, 505 F.3d 68, 71 (1st Cir. 2007) (finding that defendant’s loss in a fraud involving ATM withdrawals, was not limited to the loss that he caused, but that he, as a member of the conspiracy, was responsible for the fraudulent banking activity by all conspiracy members).

In this case, in their plea agreements, each of the Defendants agreed that “Beginning on an unknown date but not later than in or about January 2019 and continuing through on or about

October 13, 2020 . . . [Defendant], *on his own, and in concert with unknown and known persons, including* [co-Defendants], agreed to and did engage in a scheme to defraud and to obtain money by means of materially false and fraudulent pretenses, representations, and promises” Each of the Defendants agreed that the criminal activity was done individually and in concert with the other co-defendants, and each agreed that they were involved from the identified start date through their arrests. This Court should not permit the Defendants to walk back from the agreements that they have made in their plea agreements.

Next, due to the difficulty in determining the attempted loss, namely identifying each and every fraudulent claim, in every state, that was submitted by the co-Defendants and their co-conspirators (including rejected claims), the parties agreed upon a loss amount. That loss amount represented the amount of fraudulently obtained funds deposited into bank accounts identified through the investigation, including accounts associated with the debit cards recovered during the search of the Defendants’ homes. The loss in this case is not inflated, in any respect. It is a conservative estimate of loss.

Finally, in two recent, similar COVID-19 unemployment insurance fraud cases, sentencing courts rejected the same argument now made by Defendants TONY MERTILE and JUNIOR MERTILE. *See United States v. Miller*, 21-CR-411 (WFK), 2024 WL 2178974, at *2, 4 (E.D.N.Y. May 14, 2024) (rejecting the defendant’s claim the he should only be responsible for the \$255,212 loss he caused, not the \$1.75 million loss of the conspiracy of which he was a part; finding “the Court agrees with the Government that Defendant “is appropriately held responsible for losses he personally caused, as well as those he aided and abetted, and those within the scope of jointly undertaken criminal activity.”); *United States v. Golding*, Case No. 22-CR-143 (WFK), 2024 WL 2178962, *6 (E.D.N.Y. May 13, 2024) (rejecting defendant’s efforts to have only the loss

attributable to his actions considered his loss amount; finding that “[t]he more than \$1.5 million in unemployment benefits obtained by Defendant and his co-defendants was within the scope of the jointly undertaken criminal scheme to fraudulently submit claims for unemployment benefits utilizing third parties’ PII. The actual loss associated with those fraudulent claims was reasonably foreseeable to Defendant.”)

This Court should reject the Defendants’ efforts to minimize the scope of their fraud and their responsibility.

II. SENTENCING RECOMMENDATION

The sentences recommended by the Government is a significant, and a “sufficient but not greater than necessary” sentence, taking into account all of the 18 U.S.C. § 3553(a) sentencing factors, the Congressional mandate that the sentence for Aggravated Identity Theft, 18 U.S.C. § 1028A, and case law re 1028A.

A. Defendants’ Conspiracy to Commit Wire Fraud Sentences Cannot Be Reduced or Lessened Due to 24 Month Sentences to be Imposed for Aggravated Identify Theft.

As a preliminary matter, the Defendants stand before the Court convicted of Conspiracy to Commit Wire Fraud and Aggravated Identity Theft. The sentence for the Aggravated Identity Theft conviction must, by statute, be 24 months consecutive to whatever sentence the Court imposes for each of the Defendants’ convictions for Conspiracy to Commit Wire Fraud.

As this Court is aware, in accordance with the penalty provision of 18 U.S.C. § 1028A and the case law interpreting that statute, a sentencing court must determine the sentence for Count 2, Conspiracy to Commit Wire Fraud, the predicate offense in this case, independent of, and without regard for, the mandatory minimum sentence to be imposed for the violation of 18 U.S.C. § 1028A, Aggravated Identity Theft (Count 9 (TONY MERTILE); Count 11 (JUNIOR METILE),

and may not discount or offset the conviction for the predicate offense due to the mandatory minimum sentence to be imposed. 18 U.S.C. § 1028A(b)(3) states that:

in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, *a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section*; and

18 U.S.C. § 1028(b)(3) (emphasis added).

The Supreme Court, First Circuit, and other Circuits have consistently recognized that a sentencing court cannot reduce or offset the sentence to be imposed on a predicate offense due to the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A. In *Dean v. United States*, the Court held that 18 U.S.C. § 924(c), another statute setting a consecutive, mandatory minimum, did not prohibit consideration of the mandatory minimum sentence when determining sentence on the predicate offense. However, the Court expressly recognized the difference in the statutory language of 18 U.S.C. § 1028A and 18 U.S.C. § 924(c), and found that 18 U.S.C. § 1028A did not afford sentencing courts the same discretion as courts had under 18 U.S.C. § 924(c).

Congress has shown just that in another statute, 18 U.S.C. § 1028A. That section, which criminalizes the commission of identity theft “during and in relation to” certain predicate felonies, imposes a mandatory minimum sentence “in addition to the punishment provided for” the underlying offense. § 1028A(a)(1). It also says that the mandatory minimum must be consecutive to the sentence for the underlying offense. § 1028A(b)(2). So far, § 1028A tracks § 924(c) in relevant respects. But § 1028A goes further: It provides that in determining the appropriate length of imprisonment for the predicate felony “a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section.” § 1028A(b)(3).

Dean vs. United States, 581 U.S. 62, 70 (2017). The First Circuit has also recognized this statutory mandate, finding that a sentencing court may not consider the mandatory minimum sentence to be

imposed under 18 U.S.C. § 1028A, when determining the sentence for enumerated predicate offenses, such as Conspiracy to Commit Wire Fraud. *See United States v. Vidal-Reyes*, 562 F.3d 43, 54 (1st Cir. 2009) (holding that sentencing courts has authority to consider the § 1028A mandatory minimum sentence when determining sentences for non-predicate offenses, but not for predicate offenses). As the First Circuit observed, “a major concern of § 1028A(b)(3)’s drafters was to ensure, by making the sentences truly cumulative, that prosecutors had an incentive to charge both the aggravated identity theft violation and the underlying predicate felony or felonies.” *Id.* (construing H.R.Rep. No. 108-528, at 10, to show that the bill amended Title 18 to provide for a “mandatory consecutive penalty enhancement of 2 years for any individual who knowingly transfers ... the means of identification of another person in order to commit a serious Federal predicate offense”). Other Circuits have held the same. The Third Circuit has held that:

There is no doubt that § 1028A(b)(3) “bar[s] consideration of a mandatory minimum” during sentencing for the predicate felony.⁹ The Supreme Court as well as the First, Seventh, Eighth, Ninth, and Tenth Circuits have explained that under § 1028A, a sentencing court cannot reduce the sentence it would have otherwise imposed on a predicate conviction because of the knowledge of a defendant’s two-year mandatory minimum sentence for aggravated identity theft.

United States v. Yusuf, 781 Fed. Appx. 77, 80 (3rd Cir. 2019) (unpublished) (vacating sentencing and remanding; finding that the district court improperly considered the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A when imposing sentence on the predicate offense). Similarly, the Tenth Circuit found that:

Indeed, we indicated in [*United States v. Smith*, 756 F.3d 1179, 1185–87 (10th Cir. 2014)] that § 1028A(b)(3)’s plain language “does” precisely “what it says”: it “prevent[s] a sentencing court from taking account of § 1028A[(a)(1)]’s mandatory minimum[] when considering a sentence for predicate offenses” such as bank fraud. And we noted in *Smith* that our sister circuits have reached the same conclusion. . . . Thus, we hold that § 1028A(b)(3) prohibited the district court *437 from considering § 1028A(a)(1)’s two-year sentence for aggravated identify theft in crafting Lara’s sentences for bank fraud.

United States v. Lara, 733 Fed. Appx. 433 (10th Cir. 2018) (unpublished) (same) (collecting cases).

B. Nature and Circumstances of the Offense (18 U.S.C. § 3553(a)(1))

The “nature and circumstances of the offense” are egregious and compelling and warrant a significant, lengthy period of incarceration.

For most Americans, the COVID-19 pandemic resulted in an unprecedented time of financial hardship, turmoil, and suffering, but for the Defendants and their conspirators, it constituted a lucrative opportunity to enrich themselves with funds intended for unemployed workers. While most individuals were sheltering in place, taking care of loved ones, and often making tough financial sacrifices, the Defendants and their co-conspirators collaborated amongst themselves, and with others, to take advantage of programs meant to help those in need and did so for their own selfish purposes. The Defendants’ conduct victimized numerous government entities, and countless individuals, whose personal identifying information (PII) was used by the Defendants and their co-defendants.

As the pandemic ravaged the country, Congress appropriated billions of dollars to create or supplement government relief programs. Because this assistance was desperately needed by unemployed workers, independent contractors, nonprofits, and small businesses for their survival, the government made a policy decision to deliver the relief on an unprecedented scale as quickly as possible. In the spring of 2020, Congress passed the Coronavirus Aid, Relief and Economic Security (CARES) Act, which provided for a variety of economic benefits to struggling Americans during a time of severe negative economic impact as a result of the COVID-19 pandemic. At the time, the federal government had taken several steps to mitigate the effects of the pandemic on businesses and workers. The Families First Coronavirus Response Act (FFCRA) and Coronavirus

Aid, Relief, and Economic Security (CARES) Act provided additional funding to assist workers who were unemployed/had hours cut as a direct result of the COVID-19 pandemic. The money was distributed to the state workforce agencies (SWAs) which handled the disbursement of traditional (state) Unemployment Insurance (UI) benefits, and the SWA disbursed the additional federal benefits. The CARES Act allowed states to expand the scope of workers who were eligible to receive state UI benefits, to extend the period of time for which workers could be eligible for UI benefits, and to allow workers who may have exhausted UI benefits under traditional programs to receive benefits. The CARES Act further expanded the ability of states to provide benefits to unemployed workers by creating three new unemployment programs, namely, the Pandemic Unemployment Assistance (PUA) program, which permitted states to provide benefits to individuals who were self-employed, seeking part-time employment, or otherwise would not qualify for regular unemployment benefits; the Federal Pandemic Unemployment Compensation (FPUC) program, which provided an additional benefit, initially in the amount of \$600 and later, in the amount of \$300, in federal benefits to individuals collecting traditional UI program benefits or PUA benefits; and the Pandemic Emergency Unemployment Compensation (PEUC) program, which provided additional weeks of benefits for individuals who had otherwise exhausted their entitlement to regular UI benefits (collectively referred to herein as “expanded pandemic UI benefits”). This legislation was much needed, as millions of unemployed workers across the United States turned to the unemployment insurance program as their jobs were imperiled by the effects of the pandemic.

It was within this backdrop that the conspirators concocted and executed a scheme to unjustly divert finite unemployment insurance benefits from unemployed workers to themselves. Exploiting vulnerabilities in the execution of this massive relief effort, the Defendants and their

conspirators devised and repeatedly executed a fraud scheme targeting COVID-19 reliefs, including the Pandemic Unemployment Assistance Program. Specifically, the Defendants and their conspirators:

- obtained through various means the PII, including dates of birth and Social Security numbers, of identity theft victims;
- in preparation of submitting fraudulent applications to various state workforce agencies for unemployment benefits, the conspirators created and maintained email accounts to facilitate communications with state workforce agencies in the names of those for whom the conspirators had obtained PII;
- filed materially false and misleading unemployment applications with multiple state workforce agencies using the PII of identity theft victims in their possession, and on these applications, the conspirators provided fabricated employment and wage history, along with false contact information, such as physical and mailing addresses, email addresses, and phone numbers that did not, in fact, belong to the purported applicant;
- falsely certified the truth and accuracy of all the information included in the aforementioned applications, such as the purported applicants' eligibility to receive the benefits when, in truth and in fact, the conspirators then and there well knew that the information was not true and accurate, the purported claimants were not eligible for the requested benefits, and those benefits were actually being paid to conspirators and not the purported claimants;
- opened and created bank accounts using the PII of identity theft victims, and obtained debit cards for those bank accounts, and directed the state workforce agencies to directly deposit the benefit payments to the bank accounts in the names of others and/or in bank accounts controlled by them;
- once their fraudulent applications were approved, the conspirators kept, maintained, and shared amongst themselves possession of the prepaid debit cards loaded with benefit payments, and the conspirators distributed the fraud proceeds amongst themselves and others; and
- for many of the approved applications, the conspirators would often double down on, and repeat their fraud by submitting weekly recertifications of unemployment status to the state workforce agencies, falsely claiming that the purported claimant was still unemployed and entitled to receive additional unemployment benefits.

Given the scope of and means by which the Defendants and their co-conspirators committed this massive fraud, the Government was unable to fully identify the full amount of actual and attempted

losses. However, the Government was able to determine, through analysis of bank records, and the parties have agreed to a loss amount of \$4,857,191, which is based on the actual loss amount determined from review of a myriad of bank records. Therefore, the Defendant stands before this Court for being part of a conspiracy that stole nearly \$5 million.

As laid out above and in the PSR, the conspirators' scheme was labor intensive, sophisticated, and multifaceted – recruiting co-conspirators and other participants to aid in their enormous fraud, obtaining PII through various means, maintaining and distributing the PII information amongst members of the conspiracy, preparing and submitting fraudulent applications for hundreds of purported claimants, recertifying fraudulent applications on a weekly basis, creating and maintaining email accounts to facilitate communications with the state workforce agencies, forging and falsifying documents to substantiate the false information provided in the fraudulent applications, and maintaining and distributing prepaid debit cards and the fraud proceeds amongst the members of the conspiracy. The repetitive, continuous nature of the fraud makes clear that the conspirators' criminal conduct was not a product of a momentary lapse of judgment; instead, it was a rational, deliberate choice that the conspirators knowingly and willfully made over and over again. The volume, duration, and scope of the conspirators' scheme is staggering and indicative of the greed motivating the conspirators' criminal conduct.

By looting the unemployment program, the conspirators repeatedly stole finite funds from those who needed it the most during the pandemic, and their relentless pursuit of these funds showed a callous disregard to unemployed workers, identity theft victims, state workforce agencies – who had the daunting task of administering an unprecedented relief effort – and American taxpayers, whose earnings underlie the funds in question. Through their criminal conduct, the conspirators interfered with and undermined the federal government's efforts to provide necessary

and urgent relief to Americans harmed by the pandemic. The nature and circumstances of the offense well support a substantial sentence for each conspirator.

The evidence recovered from Defendants' TONY MERTILE and JUNIOR MERTILE's homes, and from the homes of their co-defendants, home, as well as review of bank records for accounts associated with the Defendants (fraudulently opened accounts and accounts in their names) show that the Defendants and their co-conspirators, had been using fraudulently obtained PII to obtain fraudulent payment from multiple federal and state government agencies *prior to* the pandemic, as early as January 2019.¹³ As a result, the when the COVID-19 pandemic began, the Defendants used their knowledge, and established systems, to defraud the Government programs to aid those struggling with COVID-19 pandemic.¹⁴

Defendants TONY MERTILE, JUNIOR MERTILE, and their co-conspirators used a network of bank accounts to steal at least \$4.8 million in COVID-19 relief funds and other government program funds, and to pass the fraud proceeds through various accounts and to each other. When search warrants were executed at the homes of the 4 co-Defendants, investigators recovered a total of 994 debit cards from multiple banks, shown below, most of which were in the names of third parties and had been used to obtain fraudulent expanded pandemic UI benefits.

¹³ The Defendants each agreed that their criminal conduct between on an unknown date but not later than in or about January 2019. See Plea Agreements, ¶ 4a.

¹⁴ In their Plea Agreements, each of the Defendants have agreed to engaging in activity "beginning on an unknown date, but not later than January 2019 and continuing through on or about October 13, 2020," which was the date of the arrests of J Legerme, T. Mertile, and J. Mertile. See Plea Agreements, ¶ 4a.

BANK	# OF CARDS
Chime	175
GoBank	295
Green Dot	229
Bank of America	61
Wells Fargo	94
Sun Trust	16
Bancorp	34
Metabank	9
BBVA	8
AMEX	23
PNC	6
Chase	6
Sutton Bank	13
Comerica	20

Lili-Choice Financial Group	1
KeyBank	1
Venmo	
Republic Bank & Trust	1
U.S. Bank	1
Navy Federal CU	1
TOTAL CARDS SEIZED	994

Moreover, ATM surveillance footage shows each of the four co-defendants, including Defendants TONY MERTILE and JUNIOR MERTILE, making ATM withdrawals using debit cards from fraudulently opened bank accounts, in other persons names, into which fraudulent expanded pandemic UI benefits were made, also in names of other persons. For many of these ATM transactions, the vehicles registered to the Defendants or spouses, or in one instance that had been rented by JUNIOR MERTILE, can be seen on the surveillance footage. Further, cell site location data for cell phones used by each of the Defendants showed that those phones were in the vicinity of ATMs when withdrawals were made from fraudulently opened account into which fraudulent UI benefit payments had been deposited. Cell site location data also shows Defendant Legerme's vehicle infotainment system in the area of fraudulent withdrawals. In the case of Defendants TONY MERTILE and Allen Bien-Aime, on at least two instances, bank surveillance footage shows them making withdrawals using the same debit card.

Examples of how Defendants TONY MERTILE and JUNIOR MERTILE, and their co-defendants used the network of bank accounts fraudulently opened and debit cards obtained in the

names of others are set forth below. The Government notes that these graphics are merely three examples of the hundreds of bank accounts opened and used by the Defendants, which were prepared in preparation for the October 2020 search warrants.

The graphic below shows the receipt of fraudulent deposits from the Rhode Island Department of Labor and Training (RIDLT) and the Internal Revenue Service (IRS) in the two SunTrust accounts opened in the name of identity theft victim C.C. From February 20, 2020 (*note: before the pandemic*) through April 2020, \$9,380 in multiple withdrawals were made from Acct-7343 (C.C.), along with account fees and a purchase. ATM surveillance footage shows that, using a debit card for the account, TONY MERTILE withdrew funds from Acct-7343 (C.C.) on March 11, 2020 and that Allen Bien-Aime withdrew funds from Acct-7343 (C.C.) April 24, 2020.

C.C. Transactions

Incoming Funds x7376		
Statement Date	Type	Amount
2/20/2020	IRS TREAS 310 TAX REF	\$ 340
3/11/2020	IRS TREAS 310 TAX REF	\$ 350
4/14/2020	RIDLT-UI	\$ 939
4/21/2020	RIDLT-UI	\$ 939
4/21/2020	RIDLT-UI	\$ 1,173
4/28/2020	RIDLT-UI	\$ 1,173
Total		\$ 4,914




C.C.
Acct x7376
Period: 02/20/20-04/30/20
Prior Balance: \$10.00



Intra-Bank Transfers			
Statement Date	Amount Out x7376	Amount In x7343	
2/20/2020	\$ (340)	\$ 340	
3/11/2020	\$ (340)	\$ 340	
3/16/2020	\$ (10)	\$ 10	
4/14/2020	\$ (909)	\$ 909	
4/15/2020	\$ (23)	\$ 22	
4/21/2020	\$ (2,100)	\$ 2,100	
4/28/2020	\$ (1,000)	\$ 1,000	
Total	\$ (4,721)	\$ 4,721	



C.C.
Acct x7343
Period: 02/20/20-04/30/20
Prior Balance: \$5.00



Incoming Funds x7343				
Statement Date	Transaction Date	Type	Location	Amount
3/11/2020		IRS TREAS 310 TAX REF		\$ 325.00
4/1/2020	4/1/2020	ATM CASH DEPOSIT	DAVIE FL	\$ 20.00
4/8/2020	4/8/2020	ATM CASH DEPOSIT	PEMBROKE PINES FL	\$ 30.00
4/14/2020		RIDLT-UI		\$ 1,090.00
4/21/2020		RIDLT-UI		\$ 989.00
4/21/2020		RIDLT-UI		\$ 1,090.00
4/21/2020		RIDLT-UI		\$ 1,186.00
4/28/2020		RIDLT-UI		\$ 1,049.00
4/28/2020		RIDLT-UI		\$ 1,090.00
4/28/2020		RIDLT-UI		\$ 1,166.00
4/30/2020		INTEREST		\$ 0.01
Total				\$ 8,065.01

Outgoing Funds x7343				
Statement Date	Transaction Date	Type	Location	Amount
2/21/2020	2/20/2020	ATM CASH WITHDRAWAL	PEMBROKE PINES PEMBROKE PINEFL	\$ (300)
2/28/2020		MONTHLY MAINTENANCE FEE		\$ (20)
3/12/2020	3/11/2020	ATM CASH WITHDRAWAL	PEMBROKE PINES PEMBROKE PINEFL	\$ (650)
3/31/2020		MONTHLY MAINTENANCE FEE		\$ (20)
4/6/2020		INTUIT TURBO TAX		\$ (30)
4/14/2020	4/14/2020	ATM CASH WITHDRAWAL	DAVIE DAVIE FL	\$ (500)
4/14/2020	4/14/2020	ATM CASH WITHDRAWAL	DAVIE DAVIE FL	\$ (500)
4/15/2020	4/14/2020	ATM CASH WITHDRAWAL	NSU UNIVERSITY CENTER FT LAUDERDALEFL	\$ (500)
4/15/2020	4/14/2020	ATM CASH WITHDRAWAL	NSU UNIVERSITY CENTER FT LAUDERDALEFL	\$ (500)
4/21/2020	4/21/2020	ATM CASH WITHDRAWAL	DAVIE DAVIE FL	\$ (100)
4/21/2020	4/21/2020	ATM CASH WITHDRAWAL	DAVIE DAVIE FL	\$ (800)
4/21/2020	4/21/2020	ATM CASH WITHDRAWAL	NSU UNIVERSITY CENTER FT LAUDERDALEFL	\$ (100)
4/22/2020	4/22/2020	ATM CASH WITHDRAWAL	EL MERCADO HIALEAH FL	\$ (800)
4/22/2020	4/22/2020	ATM CASH WITHDRAWAL	EL MERCADO HIALEAH FL	\$ (200)
4/24/2020	4/23/2020	ATM CASH WITHDRAWAL	SHERIDAN PLAZA HOLLYWOOD FL	\$ (800)
4/24/2020	4/23/2020	ATM CASH WITHDRAWAL	SHERIDAN PLAZA HOLLYWOOD FL	\$ (200)
4/27/2020	4/24/2020	ATM CASH WITHDRAWAL	LEHIGH ACRES DR-UP LEHIGH ACRES FL	\$ (800)
4/27/2020	4/24/2020	ATM CASH WITHDRAWAL	LEHIGH ACRES DR-UP LEHIGH ACRES FL	\$ (200)
4/27/2020	4/26/2020	ATM CASH WITHDRAWAL	THE FORUM FT. MYERS FL	\$ (500)
4/27/2020	4/26/2020	ATM CASH WITHDRAWAL	THE FORUM FT. MYERS FL	\$ (500)
4/27/2020	4/27/2020	ATM CASH WITHDRAWAL	THE FORUM FT. MYERS FL	\$ (400)
4/30/2020		PAID ITEM		\$ (500)
4/30/2020		PAID ITEM		\$ (500)
4/30/2020		MONTHLY MAINTENANCE FEE		\$ (20)
Total				\$ (9,470)

The next graphic below shows the receipt of fraudulent deposits from RIDLT and DOT/IRS in the two SunTrust accounts fraudulently opened in the name of identity theft victim C.O. From February 2020 (*note: before the pandemic*) through April 2020, \$5,060 in multiple ATM withdrawals were made from Acct-8381 (C.O.), and account fees were withdrawn from the account. SunTrust ATM surveillance footage shows that, using a debit card, TONY MERTILE withdrew funds from Acct-8381 (C.O.) on March 28 and April 21, 2020, and that Bien-Aime withdrew funds from Acct-8381 (C.O.) on April 24, 2020.

C.O. Transactions

Incoming Funds x8415		
Statement Date	Type	Amount
3/23/2020	AZ DEPT OF REV TAX REFUND	\$ 49
4/21/2020	RIDLT-UI	\$ 800
4/21/2020	RIDLT-UI	\$ 1,169
4/28/2020	RIDLT-UI	\$ 800
4/28/2020	RIDLT-UI	\$ 1,169
Total		\$ 3,987



C.O.
Acct x8415
Period: 02/01/20-04/30/20
Prior Balance: \$10.00



Intra-Bank Transfers			
Statement Date	Amount Out x8415	Amount In x8381	
3/23/2020	\$ (49)	\$ 49	
4/21/2020	\$ (1,150)	\$ 1,150	
4/21/2020	\$ (800)	\$ 800	
Total	\$ (1,999)	\$ 1,999	

Incoming Funds x8381		
Statement Date	Type	Amount
2/3/2020	ME BUREAU OF TAX TAX REFUND	\$ 711
2/20/2020	IRS TREAS 310 TAX REF	\$ 320
4/21/2020	RIDLT-UI	\$ 1,186
4/22/2020	IRS TREAS 310 TAX REF	\$ 358
4/28/2020	RIDLT-UI	\$ 1,186
4/28/2020	RIDLT-UI	\$ 1,186
Total		\$ 4,947



C.O.
Acct x8381
Period: 02/01/20-04/30/20
Prior Balance: \$3.00

Outgoing Funds x8381				
Statement Date	Transaction Date	Type	Location	Amount
2/10/2020	2/8/2020	ATM CASH WITHDRAWAL	WEST MIRAMAR MIRAMAR FL	\$ (500)
2/10/2020	2/9/2020	ATM CASH WITHDRAWAL	PINES AT PARAISO PEMBROKE PINEFL	\$ (200)
2/21/2020	2/20/2020	ATM CASH WITHDRAWAL	MIRAMAR MIRAMAR FL	\$ (300)
3/16/2020		MAINTENANCE FEE		\$ (7)
3/30/2020	3/28/2020	ATM CASH WITHDRAWAL	PEMBROKE PINES PEMBROKE PINEFL	\$ (60)
4/15/2020		MAINTENANCE FEE		\$ (7)
4/21/2020	4/21/2020	ATM CASH WITHDRAWAL	PLANTATION TEMP SITE PLANTATION FL	\$ (500)
4/22/2020	4/22/2020	ATM CASH WITHDRAWAL	MIAMI LAKES MIAMI LAKES FL	\$ (500)
4/23/2020	4/23/2020	ATM CASH WITHDRAWAL	THE FORUM FT MYERS FL	\$ (500)
4/27/2020	4/24/2020	ATM CASH WITHDRAWAL	RIVERSIDE DRIVE UP MIAMI FL	\$ (500)
4/27/2020	4/26/2020	ATM CASH WITHDRAWAL	LEHIGH ACRES DR-UP LEHIGH ACRES FL	\$ (500)
4/27/2020	4/27/2020	ATM CASH WITHDRAWAL	LEHIGH ACRES DR-UP LEHIGH ACRES FL	\$ (500)
4/28/2020	4/28/2020	ATM CASH WITHDRAWAL	METRO PARKWAY FORT MYERS FL	\$ (500)
4/30/2020		PAID ITEM		\$ (500)
Total				\$ (5,074)

The third graphic shows the receipt of fraudulent deposits from RIDLT and DOT in the two SunTrust accounts fraudulently opened in the name of identity theft victim R.C. From January 29, 2020 (*note: before the pandemic*) through April 2020, \$5,900 in withdrawals were made from Acct-4445 (R.C.) in multiple transactions. As shown below, JUNIOR MERTILE was observed making multiple ATM withdrawals from Acct-4445 (R.C.) on April 14, 15, 21, and 22, 2020.

MERTILE's home, in bags and boxes, would be equal to approximately 15 years of income from his reported business.

- A large collection of jewelry with an estimated value over \$250,000 including gold chains, Rolex watches, and rings. *See Exhibits 6-7.*
- A large number of debit cards in the name of other persons, from multiple banks, Chime Bank, Wells Fargo bank, SunTrust bank. *See Govt. Exhibits 14-17.*
- Multiple flip style cell phones marked with telephone numbers, including with Rhode Island area code (401), and what appeared to be a pin taped to each phone. *See Exhibits 10-13.*
- A notebook / ledger that appears to identify Green Dot and Go Bank accounts, among others, to which fund were deposited, uploaded, closed, and sent. *See Exhibit 8.*
- Checks from Sun Trust in the names of other persons, including persons whose names were used to open fraudulent Sun Trust accounts and into which fraudulent RIDLT UI benefits were directed. *See Exhibits 18-19.*
- 5 firearms. One gun was found under the front seat of his vehicle, two guns were found in a kitchen cabinet, and 2 guns were found in a crawl space in the closet of the bedroom. *See Exhibit 20.* Three children were present in the house with these unsecured firearms – an infant, a 3 year old, and a six year old.

Selected images of the items seized from TONY MERTILE's residence are copied below, and a fuller set of images will be filed under seal (due to the PII within the exhibits) as Government Exhibits 1-20.

From TONY MERTILE's Residence





At JUNIOR MERTILE's residence, among the evidence seized, investigators founds:

- \$141,038.00 in U.S. currency and a currency counting machine;
- Flip phones and multiple iPhones, and other digital devices;
- Multiple Chime and GoBank debit cards, including in the names of others; and a notebook containing PII.

Images of some of the items seized from JUNIOR MERTILE's residence, including debit cards, are copied below.

From JUNIOR MERTILE's Residence





In addition, text messages recovered from cell phones seized during the searches of all co-Defendants showed many text messages between them in which they discussed details of the fraud scheme and exchange PII of identity theft victims. Although a summary of these messages has been described in the PSR at ECF 181, PSR (TONY MERTILE), ¶¶ 41-43; ECF 174, PSR (JUNIOR MERTILE), ¶¶ 44-46, the Government has attached excerpts of the text messages in which Defendants TONY MERTILE and JUNIOR MERTILE discuss the fraud and share information with each other and with co-conspirators. These Exhibits are submitted under seal due to the PII contained therein. Exhibits 21 (Excerpts of Text Messages between TONY MERTILE and JUNIOR MERTILE), 22 (Excerpts of Text Messages between TONY MERTILE and James Legerme), and 23 (Excerpts of Text Messages between TONY MERTILE and Allen Bien-Aime).

Finally, the full means by which the Defendants obtained PII of hundreds of individuals will probably never be fully known. However, as set forth in the PSRs, during execution of the search warrant on Defendant Legerme's home, a PNC debit card in the name of a victim of identity theft, R.S. was recovered. The investigation showed that the PNC card in the name of R.S. was used to purchase access to accounts with Been Verified and Intelius, services through which

persons can purchase PII. For example, the following accounts were created: Intelius LLC / People Connect (in the name of Allen Bien-Aime) created on December 31, 2018; from Intelius LLC / People Connect (in the name of R.S. created on 8/30/2019), and Been Verified (in the name of R.S. created on August 30, 2019).

C. Need to Afford General and Specific Deterrence (18 U.S.C. § 3553(a)(2)(B))

Under 18 U.S.C. § 3553(a)(2)(B), there is a need “to afford adequate deterrence to criminal conduct.” A significant sanction needs to be imposed to send a signal to others who would contemplate engaging in wire fraud and aggravated identity theft, and to this Defendant to never return to this type of criminal activity. In this respect, the Government submits that for each of the Defendants a low-end Guideline sentence on Count 2, followed by the consecutive, mandatory 24-month term for the Aggravated Identity Theft count (Count 9 (TONY MERTILE); Count 11 (JUNIOR METILE) is appropriate in this case.

General deterrence is particularly important sentencing factor in fraud cases such as this one because it is viewed to be effective. The deliberate nature of fraud often renders it more difficult to uncover, since individuals engaged in fraud take affirmative steps to conceal their identities and conduct. The First Circuit, among others, has “emphasized the importance of general deterrence of white collar crime.” *United States v. Prosperi*, 686 F.3d 32, 47 (1st Cir. 2012); *see also United States v. Mueffelman*, 470 F.3d 33, 40 (1st Cir. 2006) (stating that “the deterrence of white collar crime” was “of central concern to Congress”); *also United States v. Landry*, 631 F.3d 597, 607 (affirming wire fraud and aggravated identify theft sentence; finding that the district court did not err in considering the need for the sentence to afford deterrence in an aggravated identity theft case); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (“Because economic and fraud-based crimes are ‘more rational, cool, and calculated than sudden crimes of passion or

opportunity’ these crimes are ‘prime candidates for general deterrence.’ ” *quoting* Stephanos Bibas, White-Collar Plea Bargaining and Sentencing After Booker, 47 Wm. & Mary L. Rev. 721, 724 (2005)).

The COVID-19 pandemic and programs created to aid struggling Americans citizens, residents, and businesses, led to a surge in identity theft and fraud against government programs in 2020 and thereafter, resulting in estimated hundreds of billions of total losses.¹⁵ Despite its best efforts, law enforcement will not ever be able to identify, catch, and convict all of the opportunistic fraudsters who made off with taxpayers’ funds during the pandemic. The case against these Defendants, and their co-conspirators, presents a worthwhile opportunity for the Court to impose a sentence that will grab the attention of those who may be considering similar crimes. The recommended sentence of imprisonment for this fraud scheme is “sufficient, but not greater than necessary” to deter this Defendant, and other who may consider engaging in similar conduct.

D. Need to Reflect the Seriousness of the Crimes, Promote Respect for the Law, and Need to Provide Just Punishment (18 U.S.C. § 3553(a)(2)(C))

The Defendants’ crimes are unquestionably serious. During the height of the COVID-19 pandemic, the Defendants’ and their conspirators countlessly executed a fraud scheme targeting state workforce agencies that were administering COVID-19 relief to unemployed workers. The conspirators unjustly diverted at least \$4,857,191 in unemployment benefits from overburdened government agencies and desperate, unemployed workers to themselves. By numbers alone, the criminal conduct is extremely serious, but the harm in this case cannot be measured solely by

¹⁵ See Richard Lardner et al, The Great Grift: How billions in COVID-19 relief aid was stolen or wasted, Associated Press, June 12, 2023, <https://apnews.com/article/pandemic-covid19-fraud-small-business-inspector-general-7e651b3e405863f0be9f2e34ca47b93e>

financial losses. The defendants' criminal conduct imposed other non-pecuniary harms on primary and secondary victims.

First, by flooding state workforce agencies with hundreds upon hundreds of fraudulent unemployment applications, the defendant raised administrative costs for these agencies, likely delaying the approval of legitimate applications by unemployed workers. This harm is far from theoretical. Facing lengthy delays in the adjudication of unpaid claims, genuinely unemployed workers initiated class action litigation against the VEC during the pandemic in order to obtain unemployment benefits owed to them in a timely manner. As United States District Court Judge Henry E. Hudson aptly observed in the separate class action on this matter, "the unprecedented COVID-19 pandemic and pandemic-related restrictions caused a significant increase in unemployment claims and overwhelmed unemployment compensation programs nationwide, including in Virginia." *Cox et al. v. Hess*, Case No. 3:21-cv-253-HEH, Dkt. No. 25 at 1 (Order). The Defendants' sentences must reflect the harm to unemployed workers who suffered lengthy delays in the approval of their legitimate unemployment claims and the receipt of much needed benefits due to the increase in administrative costs on state workforce agencies caused by the conspirators' submission of numerous fraudulent applications.

Second, although the identity theft victims in this case did not directly suffer a financial loss to the Government's knowledge, being the victim of identity theft is truly a life altering experience, nonetheless. In addition to potential financial harm, many victims of identity theft suffer devastating emotional and psychological trauma from these crimes, resulting in feelings of anger, fear, anxiety, depression, confusion, and more. Moreover, the conspirators filing claims using the PII of identity theft victims potentially hampered the ability of these individuals to obtain

unemployment benefits and created potential tax liabilities for victims who never knew of or received the unemployment benefits obtained in their names.

Fourth and finally, while the state workforce agencies and identity theft victims are the ostensible victims in this case, the Defendants and their co-conspirators also defrauded American taxpayers whose earnings underlie the government program in question. In sum, the Defendants' crimes are serious and deserving of a lengthy term of imprisonment.

E. Need to Avoid Unwarranted Sentencing Disparities (18 U.S.C. § 3553(a)(6))

Under 18 U.S.C. § 3553(a)(6), there is a need to “avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct.” “Section 3553(a)(6) ‘is primarily aimed at national disparities, rather than those between co-defendants.’” *United States v. Reyes-Rivera*, 812 F.3d 79, 90 (1st Cir. 2016) (affirming 242 month sentence for \$22 million Ponzi scheme) (citing *United States v. Marceau*, 554 F.3d 24, 33 (1st Cir.2009)). *See also United States v. Munyenyezi*, 781 F.3d 532, 545 (rejecting claim that disparity refers to disparity among sentences within a district; finding that 18 U.S.C. § 3553(a)(6) “primarily refers to national disparities among similarly situated defendants.”)

Within this District, conspiracy to commit wire fraud cases are not novel. However, the backdrop of the COVID-19 crisis in the United States is unique. Although other cases involving UI fraud during the COVID-19 pandemic have proceeded to sentencing in this District, none of those cases came close to approaching the magnitude and sophistication of the fraud committed by this group of defendants has been sentenced in this District. In a review across the country as to how various districts have sentenced COVID-19 related fraud cases committed during a time of national crisis, several cases are consistent with the Government's recommendation here and have yielded significant sentences. *See, e.g., United States v. Jerry Phillips*, TDC-22-073 (D. Maryland

2023), the defendant and his co-defendant, Jaleel Phillips,¹⁶ was sentenced to 84 months (60 months + 24 months) for fraud involving pandemic UI benefits, CARES Act Paycheck Protection Program (PPP) loan applications, and Economic Injury Disaster loan (EIDL) applications); *United States v. Kenny Lee Howard*, 24-cr-20142-LVP-DRG, (EDMI, March 13, 2025) (sentenced to 94 months wire fraud and aggravated identity theft for role in COVID-19 UI fraud with \$6.2 million loss (actual), and in excess of \$11 possible); *United States v. Heather Huffman*, 22-cr-00008-JAG-MRC, (E.D. Va. 2024) (former federal employee sentenced to 216 months for wire fraud and aggravated identity theft in COVID-19 UI fraud with \$3.5 million attempted loss and \$2 million actual loss); *United States v. Beaty*, No. 23-2060, 2024 WL 5003232 (6th Cir. December 6, 2024) (affirming W.D.M.I. sentence; defendant sentenced to 124 months (84 months for conspiracy to commit wire fraud + 24 months for aggravated identity theft) for UI (\$760K) and SBA loan fraud (\$300K)); *United States v. Gladstone Njokem*, RDB-21-338 (D. Maryland 2023) (sentencing defendant to 54 months for conspiracy to commit wire fraud and aggravated identity theft for \$1.3M UI fraud with 183 PII victims); *United States v. Eric Michael Jaklitsch*, 22-cr-00015-WBS-1 (EDCA) (sentenced to 81 months (57 months + 24 months) for \$7.5 million UI and Economic Injury Disaster Loan (EIDL) fraud); *United States v. Joseph Marsell Cartlidge, Eric Alexander McMiller, and David Christopher Redfern*, 1:20-CR-340 (M.D.N.C. 2022) (receiving 72 months, 66 months, and 60 months of imprisonment, respectively for submitting fraudulent PPP and EIDL applications, obtaining \$1.2M in loans); *United States v. Lola Kasali*, 4:20-MJ-1106 (S.D. Tex. 2022) (receiving 70 months of imprisonment for submitting two fraudulent PPP loan applications and obtaining \$1.9M in loans); *United States v. Tarik Freitekh*, 3:20-CR-00435 (W.D.N.C. 2022)

¹⁶ The Government notes that defendant Jerry Phillips had a machine gun in his possession at the time of his arrest, which he had purchased as a “ghost gun” and modified.

(receiving 87 months of imprisonment for submitting fraudulent PPP applications and obtaining \$1.75M in loans); *United States v. Adam D. Arena*, 21-MJ-05134 (W.D.N.Y. 2022) (receiving 66 months of imprisonment for his role in fraudulently obtaining and laundering approximately \$950,000 in pandemic loans).

F. Need to Protect the Public (18 U.S.C. § 3553(a)(2)(C))

When fashioning an appropriate sentence, the Court must also consider protecting the public from further crimes committed by the defendant. 18 U.S.C. § 3553(a)(2). A low-end Guideline sentence on Count 2, followed by the consecutive, mandatory 24-month term for the Aggravated Identity Theft count (Count 9 (TONY MERTILE); Count 11 (JUNIOR METILE) is appropriate in this case, will protect the public from future crimes of the defendant and will promote respect for the law.

III. CONCLUSION

For all of these reasons, the Government urges this Court to impose the recommended sentences for each of the Defendants

Respectfully submitted,

SARA MIRON BLOOM
ACTING UNITED STATES ATTORNEY



DENISE M. BARTON
STACEY A. ERICKSON
Assistant U.S. Attorneys
JOHN MOREIRA
Special Assistant U.S. Attorney
United States Attorney's Office
One Financial Plaza, 17th Floor
Providence, RI 02903
401-709-5000 (office)

CERTIFICATE OF SERVICE

I hereby certify that on this 18 day of March 2025, I caused the within
GOVERNMENT’S COMBINED SENTENCING MEMORANDUM FOR DEFENDANTS
TONY MERTILE and JUNIOR MERTILE to be filed electronically and to be available for
downloading on the Court’s ECF system:

A handwritten signature in blue ink that reads "Denise M. Barton". The signature is cursive and fluid.

DENISE M. BARTON
Assistant U. S. Attorney,
U. S. Attorney's Office
One Financial Center Plaza, 17th Floor
Providence, RI 02903
401-709-5000

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA

CR. No.: 20-CR-0020-MRD

v.

ALLEN BIEN-AIME,
Defendant.

GOVERNMENT’S SENTENCING MEMORANDUM

In accordance with the plea agreement, and for the reasons set forth herein, the Government asks the Court to impose a low-end Guideline sentence of imprisonment¹ of 102 months imprisonment for Defendant Allen Bien-Aime (Bien-Aime); enter an order of restitution for \$4,456,927.36; and grant the Motion for Order of Forfeiture (Money Judgment)² in the amount of \$1,214,294.75. Having previously been federally convicted for a similar offense, Defendant Bien-Aime engaged in a carefully orchestrated fraud and identify theft scheme, with his co-conspirator co-defendants that targeted relief designed to aid those in need during the COVID-19 pandemic, and stole at least \$4.8 million.

¹ The Presentence Report currently calculates the Guideline range as 78-87 months for Count 2 (Conspiracy to Commit Wire Fraud), plus a consecutive 24 months for Count 7 (Aggravated Identity Theft), for a combined Guideline range of 102-111 months. ECF 172, Presentence Report, ¶ 114. The Defendant has objected to the application of a +2 enhancement under U.S.S.G. 2B1.1(b)(11). The Probation Department has responded that the enhancement is appropriate, and the Government agrees for the reasons set forth herein. However, if the Defendant’s objections are sustained, the Guideline range may change. If the Guideline range changes, the Government will amend its sentencing recommendation at the Sentencing Hearing, to make the agreed-upon low-end Guideline recommendation.

² As set forth in ECF 166, in the Government’s Motion For Order Of Forfeiture (Money Judgment), in his Plea Agreement, the Defendant agreed that an amount of \$4,857,191 constitutes proceeds of the conspiracy charged in Count 2, and that that he will forfeit a sum of money in the amount of \$1,214,294.75 in the form of a forfeiture money judgement.

I. OUTSTANDING OBJECTIONS

In considering objections and determining what guideline adjustments apply, the Court must find that the Government has made a showing of any fact necessary and relevant to sentencing by a preponderance of the evidence. *United States v. Flete-Garcia*, 925 F.3d 17, 28 (1st Cir. 2019). The Court has “considerable discretion” in determining what evidence should be regarded as reliable for such fact-finding. *Id.* at 28. Because at the sentencing phase a defendant has no right to confront witnesses against him and sentencing courts may rely on hearsay evidence, *see United States v. Rodriguez*, 336 F.3d 67, 71 (1st Cir. 2003), the Court may appropriately rely on documentary information such as the PSR, affidavits, exhibits, and submissions of counsel. *United States v. Curran*, 525 F.3d 74, 78 (1st Cir. 2008) (quoting *United States v. Ranney*, 298 F.3d 74, 81 (1st Cir.2002)). The Court may “evaluate virtually *any* dependable information” to determine the probative value of such information with respect to issues material to sentencing. *United States v. Bradley*, 917 F.2d 601, 605 (1st Cir. 1990) (emphasis added); *see, e.g., United States v. Acevedo-Lopez*, 873 F.3d 330, 340 (1st Cir. 2017) (relying upon hearsay proffer of the AUSA).

The Court may consider relevant information without regard to its admissibility under the rules of evidence applicable at trial, provided that the information has sufficient indicia of reliability, U.S.S.G. § 6A1.3(a), including out-of-court statements by witnesses. *United States v. Lee*, 892 F.3d 488, 492 (1st Cir. 2018). Such indicia may include details, internal consistence, and corroboration by multiple witnesses. *United States v. Green*, 426 F.3d 64, 67 (1st Cir. 2005) (emphasis added).

Evaluation of the submitted information need not involve a hearing. Rather, “[a]t sentencing, evidentiary hearings are the exception, not the rule.” *Flete-Garcia*, 925 F.3d at 34 (citing *United States v. Shattuck*, 961 F.2d 1012, 1014-15 (1st Cir. 1992)). The parties need only

have an “adequate opportunity to present information to the court” about any sentencing factor that is “reasonably in dispute.” *Id.* at 35; U.S.S.G. § 6A1.3(a). Where the Government provides documentary support sufficient for factual findings, there is no need to “bolster” the evidence by calling a live witness. *See United States v. Gerante*, 891 F.2d 364, 367 (1st Cir. 1989).

A. Objection as to+2 Under U.S.S.G. § 2B1.1(b)(11)(A) or (B) – Possession and Use of an Authentication Feature

Defendant Bien-Aime has objected to the enhancement under U.S.S.G. § 2B1.1(b)(11)(A) at paragraph 52 of the Presentence Report (PSR). *See* ECF 172-2, Bien-Aime PSR, Addendum. In summary, he argues that the debit card is not an “authentication feature” and that the application of this enhancement is double counting. The Defendant’s argument fails on both grounds, as explained below and by the Probation Officer in his Response to the Objection. *Id.*³

First,

[t]he term “authentication feature” means any hologram, watermark, certification, symbol, code, image, *sequence of numbers* or letters, or other feature that either individually or in combination with another feature is used by the issuing authority on an identification document, document-making implement, or means of identification to determine if the document is counterfeit, altered, or otherwise falsified.

18 U.S.C. § 1028(d). During the course of their fraudulent endeavors, the co-defendants, including BIEN-AIME, had fraudulent funds deposited into fraudulently opened accounts for which they obtained debit cards. To withdraw the fraudulent proceeds, the co-defendants, including BIEN-AIME, used PIN numbers for the debit cards to withdraw funds. The PIN number, as well as any other security features on the debit cards, constitute an authentication feature.

³ The Government incorporates the Response to this Objection by the Probation Officer in ECF 172-2, as if set forth fully herein.

Next, the language of the Guidelines show that Defendant’s double-counting argument also fails. U.S.S.G. § 2B1.1(b)(11) states that an enhancement applies if the offense involved:

(A) the possession or use of any (i) device-making equipment, or (ii) authentication feature;

(B) the production or trafficking of any (i) unauthorized access device or counterfeit access device, or (ii) authentication feature; or

(C) (i) the unauthorized *transfer or use of any means of identification* unlawfully to produce or obtain any other means of identification, or (ii) the *possession of 5 or more means of identification* that unlawfully were produced from, or obtained by the use of, another means of identification,

U.S.S.G. § 2B1.1(b)(11) (emphasis added). Recognizing the potential for impermissible double counting, U.S.S.G. §2B1.6, the Guideline for the 18 U.S.C. § 1028A offense, prohibits application of specific offense conduct enhancement for “the transfer, possession, or use of a means of identification.”

If a sentence under this guideline is imposed in conjunction with a sentence for an underlying offense, do not apply any specific offense characteristic for the *transfer, possession, or use of a means of identification* when determining the sentence for the underlying offense.

U.S.S.G. § 2B1.6 (emphasis added). By its terms, that prohibition is specifically limited to specific offense conduct involving the “*transfer, possession, or use of a means of identification*,” which, for U.S.S.G. § 2B1.1(b)(11), would only include subpart (C) of that Guideline. *See United States v. James*, 744 Fed. Appx. 664, 666 (11th Cir. 2018) (“Section 2B1.6 does not bar all sentencing enhancement for defendants who are convicted under § 1028A, because not all § 1028A conduct involves only the transfer, possession, or use of another person’s means of identification.”). The First Circuit has held that U.S.S.G. § 2B1.6 does not prohibit application of an enhancement under U.S.S.G. § 2B1.1(b)(11), provided the enhancement is not based on conduct described in subpart (C) or the “trafficking” conduct in subpart (B) of U.S.S.G. § 2B1.1(b)(11), neither of which is the

basis for the enhancement in this case. *See United States v. Jones*, 551 F.3d 19, 25-26 (1st Cir. 2008) (applying +2 enhancement for production of a fraudulent license under U.S.S.G. § 2B1.1(b)(10)(B) (prior version of U.S.S.G. § 2B1.1(b)(11)(B)), and finding that trafficking of means of identification was a “transfer” of a means of identification); *United States v. Sharapka*, 526 F.3d 58, 61-62 (1st Cir. 2008) (applying +2 enhancement for use of device making equipment under U.S.S.G. § 2B1.1(b)(10)(A) (prior version of U.S.S.G. § 2B1.1(b)(11)(A))). Other Circuits have reached the same conclusion. *See United States v. Pendergrass*, No. 22-13018, 2025 WL 78172, at *9-10 (11th Cir. January 13, 2025) (recognizing that application of § 2B1.1(b)(11)(A), for use of an authentication feature, was proper, and did not constitute double-counting); *United States v. A.M.*, 927 F.3d 718, 720-21 (3rd Cir. 2019) (affirming application of +2 enhancement under subpart (A) of U.S.S.G. § 2B1.1(b)(11), which was found to be distinct from the conduct in subpart (C) of § 2B1.1(b)(11), for which the enhancement would be precluded under U.S.S.G. § 2B1.6); *United States v. Damyanov*, 503 Fed. Appx. 224, 225-26 (4th Cir. 2013) (“§ 2B1.6 does not exclude all conduct described in” U.S.S.G. § 2B1.1(b)(11);” affirming +2 enhancement under 2B1.1(b)(11)(B) based on production).

In this case, the Government agrees with the Probation Officer that the enhancement applies under U.S.S.G. § 2B1.1(b)(11)(A) (“the possession or use of any . . . (ii) authentication feature”). As described in the Probation Officer’s response, the Defendant and his co-conspirators’ conduct involved a much broader range of conduct than the conduct for which application of this enhancement would be prohibit under U.S.S.G. § 2B1.6. Moreover, the Defendant and his co-defendants possessed and used the authentication features for the debit cards which they used to withdraw fraudulent funds from the fraudulent bank accounts.

II. SENTENCING RECOMMENDATION

The sentence recommended by the Government is a significant, and a “sufficient but not greater than necessary” sentence, taking into account all of the 18 U.S.C. § 3553(a) sentencing factors, the Congressional mandate that the sentence for Aggravated Identity Theft, 18 U.S.C. § 1028A, and case law re 1028A.

A. Defendant’s Conspiracy to Commit Wire Fraud Sentence Cannot Be Reduced or Lessened Due to 24 Month Sentence to be Imposed for Aggravated Identify Theft.

As a preliminary matter, the Defendant stands before the Court convicted of Conspiracy to Commit Wire Fraud and Aggravated Identity Theft. The sentence for his Aggravated Identity Theft conviction must, by statute, be 24 months consecutive to whatever sentence the Court imposes for his conviction for Conspiracy to Commit Wire Fraud.

As this Court is aware, in accordance with the penalty provision of 18 U.S.C. § 1028A and the case law interpreting that statute, a sentencing court must determine the sentence for Count 2, Conspiracy to Commit Wire Fraud, the predicate offense in this case, independent of, and without regard for, the mandatory minimum sentence to be imposed for his violation of Count 7. Aggravated Identify Theft, and may not discount or offset the conviction for the predicate offense due to the mandatory minimum sentence to be imposed. 18 U.S.C. § 1028A(b)(3) states that:

in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

18 U.S.C. § 1028(b)(3) (emphasis added).

The Supreme Court, First Circuit, and other Circuits have consistently recognized that a sentencing court cannot reduce or offset the sentence to be imposed on a predicate offense due to the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A. In *Dean v. United*

States, the Court held that 18 U.S.C. § 924(c), another statute setting a consecutive, mandatory minimum, did not prohibit consideration of the mandatory minimum sentence when determining sentence on the predicate offense. However, the Court expressly recognized the difference in the statutory language of 18 U.S.C. § 1028A and 18 U.S.C. § 924(c), and found that 18 U.S.C. § 1028A did not afford sentencing courts the same discretion as courts had under 18 U.S.C. § 924(c).

Congress has shown just that in another statute, 18 U.S.C. § 1028A. That section, which criminalizes the commission of identity theft “during and in relation to” certain predicate felonies, imposes a mandatory minimum sentence “in addition to the punishment provided for” the underlying offense. § 1028A(a)(1). It also says that the mandatory minimum must be consecutive to the sentence for the underlying offense. § 1028A(b)(2). So far, § 1028A tracks § 924(c) in relevant respects. But § 1028A goes further: It provides that in determining the appropriate length of imprisonment for the predicate felony “a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section.” § 1028A(b)(3).

Dean vs. United States, 581 U.S. 62, 70 (2017). The First Circuit has also recognized this statutory mandate, finding that a sentencing court may not consider the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A, when determining the sentence for enumerated predicate offenses, such as Conspiracy to Commit Wire Fraud. *See United States v. Vidal-Reyes*, 562 F.3d 43, 54 (1st Cir. 2009) (holding that sentencing courts has authority to consider the § 1028A mandatory minimum sentence when determining sentences for non-predicate offenses, but not for predicate offenses). As the First Circuit observed, “a major concern of § 1028A(b)(3)’s drafters was to ensure, by making the sentences truly cumulative, that prosecutors had an incentive to charge both the aggravated identity theft violation and the underlying predicate felony or felonies.” *Id.* (construing H.R.Rep. No. 108-528, at 10, to show that the bill amended Title 18 to provide for a “mandatory consecutive penalty enhancement of 2 years for any individual who knowingly

transfers ... the means of identification of another person in order to commit a serious Federal predicate offense”). Other Circuits have held the same. The Third Circuit has held that:

There is no doubt that § 1028A(b)(3) “bar[s] consideration of a mandatory minimum” during sentencing for the predicate felony.⁹ The Supreme Court as well as the First, Seventh, Eighth, Ninth, and Tenth Circuits have explained that under § 1028A, a sentencing court cannot reduce the sentence it would have otherwise imposed on a predicate conviction because of the knowledge of a defendant’s two-year mandatory minimum sentence for aggravated identity theft.

United States v. Yusuf, 781 Fed. Appx. 77, 80 (3rd Cir. 2019) (unpublished) (vacating sentencing and remanding; finding that the district court improperly considered the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A when imposing sentence on the predicate offense). Similarly, the Tenth Circuit found that:

Indeed, we indicated in [*United States v. Smith*, 756 F.3d 1179, 1185–87 (10th Cir. 2014)] that § 1028A(b)(3)’s plain language “does” precisely “what it says”: it “prevent[s] a sentencing court from taking account of § 1028A[(a)(1)]’s mandatory minimum[] when considering a sentence for predicate offenses” such as bank fraud. And we noted in *Smith* that our sister circuits have reached the same conclusion. . . . Thus, we hold that § 1028A(b)(3) prohibited the district court *437 from considering § 1028A(a)(1)’s two-year sentence for aggravated identify theft in crafting Lara’s sentences for bank fraud.

United States v. Lara, 733 Fed. Appx. 433 (10th Cir. 2018) (unpublished) (same) (collecting cases).

A. Nature and Circumstances of the Offense (18 U.S.C. § 3553(a)(1))

The “nature and circumstances of the offense” are egregious and compelling and warrant a significant, lengthy period of incarceration.

For most Americans, the COVID-19 pandemic resulted in an unprecedented time of financial hardship, turmoil, and suffering, but for the Defendant and his conspirators, it constituted a lucrative opportunity to enrich themselves with funds intended for unemployed workers. While most individuals were sheltering in place, taking care of loved ones, and often making tough

financial sacrifices, the Defendant and his co-conspirators collaborated amongst themselves, and with others, to take advantage of programs meant to help those in need and did so for their own selfish purposes. The Defendant's conduct victimized numerous government entities, and countless individuals, whose personal identifying information (PII) was used by the Defendant and his co-defendants.

As the pandemic ravaged the country, Congress appropriated billions of dollars to create or supplement government relief programs. Because this assistance was desperately needed by unemployed workers, independent contractors, nonprofits, and small businesses for their survival, the government made a policy decision to deliver the relief on an unprecedented scale as quickly as possible. In the spring of 2020, Congress passed the Coronavirus Aid, Relief and Economic Security (CARES) Act, which provided for a variety of economic benefits to struggling Americans during a time of severe negative economic impact as a result of the COVID-19 pandemic. At the time, the federal government had taken several steps to mitigate the effects of the pandemic on businesses and workers. The Families First Coronavirus Response Act (FFCRA) and Coronavirus Aid, Relief, and Economic Security (CARES) Act provided additional funding to assist workers who were unemployed/had hours cut as a direct result of the COVID-19 pandemic. The money was distributed to the state workforce agencies (SWAs) which handled the disbursement of traditional (state) Unemployment Insurance (UI) benefits, and the SWA disbursed the additional federal benefits. The CARES Act allowed states to expand the scope of workers who were eligible to receive state UI benefits, to extend the period of time for which workers could be eligible for UI benefits, and to allow workers who may have exhausted UI benefits under traditional programs to receive benefits. The CARES Act further expanded the ability of states to provide benefits to unemployed workers by creating three new unemployment programs, namely, the Pandemic

Unemployment Assistance (PUA) program, which permitted states to provide benefits to individuals who were self-employed, seeking part-time employment, or otherwise would not qualify for regular unemployment benefits; the Federal Pandemic Unemployment Compensation (FPUC) program, which provided an additional benefit, initially in the amount of \$600 and later, in the amount of \$300, in federal benefits to individuals collecting traditional UI program benefits or PUA benefits; and the Pandemic Emergency Unemployment Compensation (PEUC) program, which provided additional weeks of benefits for individuals who had otherwise exhausted their entitlement to regular UI benefits (collectively referred to herein as “expanded pandemic UI benefits”). This legislation was much needed, as millions of unemployed workers across the United States turned to the unemployment insurance program as their jobs were imperiled by the effects of the pandemic.

It was within this backdrop that the conspirators concocted and executed a scheme to unjustly divert finite unemployment insurance benefits from unemployed workers to themselves. Exploiting vulnerabilities in the execution of this massive relief effort, the defendant and his conspirators devised and repeatedly executed a fraud scheme targeting COVID-19 reliefs, including the Pandemic Unemployment Assistance Program. Specifically, the Defendant and his conspirators:

- obtained through various means the PII, including dates of birth and Social Security numbers, of identity theft victims;
- in preparation of submitting fraudulent applications to various state workforce agencies for unemployment benefits, the conspirators created and maintained email accounts to facilitate communications with state workforce agencies in the names of those for whom the conspirators had obtained PII;
- filed materially false and misleading unemployment applications with multiple state workforce agencies using the PII of identity theft victims in their possession, and on these applications, the conspirators provided fabricated employment and wage history, along

with false contact information, such as physical and mailing addresses, email addresses, and phone numbers that did not, in fact, belong to the purported applicant;

- falsely certified the truth and accuracy of all the information included in the aforementioned applications, such as the purported applicants' eligibility to receive the benefits when, in truth and in fact, the conspirators then and there well knew that the information was not true and accurate, the purported claimants were not eligible for the requested benefits, and those benefits were actually being paid to conspirators and not the purported claimants;
- opened and created bank accounts using the PII of identity theft victims, and obtained debit cards for those bank accounts, and directed the state workforce agencies to directly deposit the benefit payments to the bank accounts in the names of others and/or in bank accounts controlled by them;
- once their fraudulent applications were approved, the conspirators kept, maintained, and shared amongst themselves possession of the prepaid debit cards loaded with benefit payments, and the conspirators distributed the fraud proceeds amongst themselves and others; and
- for many of the approved applications, the conspirators would often double down on, and repeat their fraud by submitting weekly recertifications of unemployment status to the state workforce agencies, falsely claiming that the purported claimant was still unemployed and entitled to receive additional unemployment benefits.

Given the scope of and means by which the Defendant and his co-conspirators committed this massive fraud, the Government was unable to fully identify the full amount of actual and attempted losses. However, the Government was able to determine, through analysis of bank records, and the parties have agreed to a loss amount of \$4,857,191, which is based on the actual loss amount determined from review of a myriad of bank records. Therefore, the Defendant stands before this Court for being part of a conspiracy that stole nearly \$5 million.

As laid out above and in the PSR, the conspirators' scheme was labor intensive, sophisticated, and multifaceted – recruiting co-conspirators and other participants to aid in their enormous fraud, obtaining PII through various means, maintaining and distributing the PII

information amongst members of the conspiracy, preparing and submitting fraudulent applications for hundreds of purported claimants, recertifying fraudulent applications on a weekly basis, creating and maintaining email accounts to facilitate communications with the state workforce agencies, forging and falsifying documents to substantiate the false information provided in the fraudulent applications, and maintaining and distributing prepaid debit cards and the fraud proceeds amongst the members of the conspiracy. The repetitive, continuous nature of the fraud makes clear that the conspirators' criminal conduct was not a product of a momentary lapse of judgment; instead, it was a rational, deliberate choice that the conspirators knowingly and willfully made over and over again. The volume, duration, and scope of the conspirators' scheme is staggering and indicative of the greed motivating the conspirators' criminal conduct.

By looting the unemployment program, the conspirators repeatedly stole finite funds from those who needed it the most during the pandemic, and their relentless pursuit of these funds showed a callous disregard to unemployed workers, identity theft victims, state workforce agencies – who had the daunting task of administering an unprecedented relief effort – and American taxpayers, whose earnings underlie the funds in question. Through their criminal conduct, the conspirators interfered with and undermined the federal government's efforts to provide necessary and urgent relief to Americans harmed by the pandemic. The nature and circumstances of the offense well support a substantial sentence for each conspirator.

During search warrants executed at the homes of the 4 co-Defendants, investigators recovered a total of 994 debit cards from multiple banks, shown below, most of which were in the names of third parties and had been used to obtain fraudulent expanded pandemic UI benefits. The evidence recovered from the Defendant's home, as well as review of bank records for accounts associated with the Defendant (fraudulently opened accounts and accounts in their names) show

that Defendant Bien-Aime, and his co-conspirators, had been using fraudulently obtained PII to obtain fraudulent payment from multiple federal and state government agencies prior to the pandemic. As a result, the when the COVID-19 pandemic began, the Defendants used their knowledge, and established systems, to defraud the Government programs to aid those struggling with COVID-19 pandemic.⁴

BANK	# OF CARDS
Chime	175
GoBank	295
Green Dot	229
Bank of America	61
Wells Fargo	94
Sun Trust	16
Bancorp	34
Metabank	9
BBVA	8
AMEX	23
PNC	6
Chase	6
Sutton Bank	13
Comerica	20

Lili-Choice Financial Group	1
KeyBank	1
Venmo	
Republic Bank & Trust	1
U.S. Bank	1
Navy Federal CU	1
TOTAL CARDS SEIZED	994

Communications between Defendant Bien-Aime and co-defendant T. Mertile, and images of Bien-Aime, withdrawing funds from ATMs using fraudulently obtained debit cards in the names of others, show the substantial scope of his role in this conspiracy. Due to the amount of PII in the exhibits, the text messages will be submitted under seal as Exhibit 1 to this Memorandum, and selected images of Defendant Bien-Aime withdrawing funds will be submitted under seal as Exhibit 2. *See* PSR, ¶ 40.

⁴ In their Plea Agreements, each of the Defendants have agreed to engaging in activity “beginning on an unknown date, but not later than January 2019 and continuing through on or about October 13, 2020,” which was the date of the arrests of J Legerme, T. Mertile, and J. Mertile. *See* Plea Agreements, ¶ 4a.

B. History and Characteristics of the Defendant (18 U.S.C. § 3553(a)(1))

Defendant Bien-Aime has already been convicted and sentenced in federal court, the SDFL, for a similar offense. *See* PSR, ¶ 41. Yet, notwithstanding that conviction, he was not deterred and returned to the same sort of criminal activity.

C. Need to Afford General and Specific Deterrence (18 U.S.C. § 3553(a)(2)(B))

Under 18 U.S.C. § 3553(a)(2)(B), there is a need “to afford adequate deterrence to criminal conduct.” A significant sanction needs to be imposed to send a signal to others who would contemplate engaging in wire fraud and aggravated identity theft, and to this Defendant to never return to this type of criminal activity. In this respect, the Government submits that a low-end Guideline sentence on Count 2, followed by the consecutive, mandatory 24-month term for Count 7, is justified in this case.

General deterrence is particularly important sentencing factor in fraud cases such as this one because it is viewed to be effective. The deliberate nature of fraud often renders it more difficult to uncover, since individuals engaged in fraud take affirmative steps to conceal their identities and conduct. The First Circuit, among others, has “emphasized the importance of general deterrence of white collar crime.” *United States v. Prosperi*, 686 F.3d 32, 47 (1st Cir. 2012); *see also United States v. Mueffelman*, 470 F.3d 33, 40 (1st Cir. 2006) (stating that “the deterrence of white collar crime” was “of central concern to Congress”); *also United States v. Landry*, 631 F.3d 597, 607 (affirming wire fraud and aggravated identify theft sentence; finding that the district court did not err in considering the need for the sentence to afford deterrence in an aggravated identity theft case); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (“Because economic and fraud-based crimes are ‘more rational, cool, and calculated than sudden crimes of passion or

opportunity’ these crimes are ‘prime candidates for general deterrence.’ ” *quoting* Stephanos Bibas, White-Collar Plea Bargaining and Sentencing After Booker, 47 Wm. & Mary L. Rev. 721, 724 (2005)).

The COVID-19 pandemic and programs created to aid struggling Americans citizens, residents, and businesses, led to a surge in identity theft and fraud against government programs in 2020 and thereafter, resulting in estimated hundreds of billions of total losses.⁵ Despite its best efforts, law enforcement will not ever be able to identify, catch, and convict all of the opportunistic fraudsters who made off with taxpayers’ funds during the pandemic. The case against this Defendant, and his co-conspirators, presents a worthwhile opportunity for the Court to impose a sentence that will grab the attention of those who may be considering similar crimes. The recommended sentence of imprisonment for this fraud scheme is “sufficient, but not greater than necessary” to deter this Defendant, and other who may consider engaging in similar conduct.

D. Need to Reflect the Seriousness of the Crimes, Promote Respect for the Law, and Need to Provide Just Punishment (18 U.S.C. § 3553(a)(2)(C))

The Defendant’s crimes are unquestionably serious. During the height of the COVID-19 pandemic, he and his conspirators countlessly executed a fraud scheme targeting state workforce agencies that were administering COVID-19 relief to unemployed workers. The conspirators unjustly diverted at least \$4,857,191 in unemployment benefits from overburdened government agencies and desperate, unemployed workers to themselves. By numbers alone, the criminal conduct is extremely serious, but the harm in this case cannot be measured solely by financial losses. The defendant’s criminal conduct imposed other non-pecuniary harms on primary and secondary victims.

⁵ See Richard Lardner et al, The Great Grift: How billions in COVID-19 relief aid was stolen or wasted, Associated Press, June 12, 2023, <https://apnews.com/article/pandemic-covid19-fraud-small-business-inspector-general-7e651b3e405863f0be9f2e34ca47b93e>

First, by flooding state workforce agencies with hundreds upon hundreds of fraudulent unemployment applications, the defendant raised administrative costs for these agencies, likely delaying the approval of legitimate applications by unemployed workers. This harm is far from theoretical. Facing lengthy delays in the adjudication of unpaid claims, genuinely unemployed workers initiated class action litigation against the VEC during the pandemic in order to obtain unemployment benefits owed to them in a timely manner. As United States District Court Judge Henry E. Hudson aptly observed in the separate class action on this matter, “the unprecedented COVID-19 pandemic and pandemic-related restrictions caused a significant increase in unemployment claims and overwhelmed unemployment compensation programs nationwide, including in Virginia.” *Cox et al. v. Hess*, Case No. 3:21-cv-253-HEH, Dkt. No. 25 at 1 (Order). The defendant’s sentence must reflect the harm to unemployed workers who suffered lengthy delays in the approval of their legitimate unemployment claims and the receipt of much needed benefits due to the increase in administrative costs on state workforce agencies caused by the conspirators’ submission of numerous fraudulent applications.

Second, although the identity theft victims in this case did not directly suffer a financial loss to the Government’s knowledge, being the victim of identity theft is truly a life altering experience, nonetheless. In addition to potential financial harm, many victims of identity theft suffer devastating emotional and psychological trauma from these crimes, resulting in feelings of anger, fear, anxiety, depression, confusion, and more. Moreover, the conspirators filing claims using the PII of identity theft victims potentially hampered the ability of these individuals to obtain unemployment benefits and created potential tax liabilities for victims who never knew of or received the unemployment benefits obtained in their names.

Fourth and finally, while the state workforce agencies and identity theft victims are the ostensible victims in this case, the Defendant and his co-conspirators also defrauded American taxpayers whose earnings underlie the government program in question. In sum, the Defendant's crimes are serious and deserving of a lengthy term of imprisonment.

B. Need to Avoid Unwarranted Sentencing Disparities (18 U.S.C. § 3553(a)(6))

Under 18 U.S.C. § 3553(a)(6), there is a need to “avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct.” “Section 3553(a)(6) ‘is primarily aimed at national disparities, rather than those between co-defendants.’” *United States v. Reyes-Rivera*, 812 F.3d 79, 90 (1st Cir. 2016) (affirming 242 month sentence for \$22 million Ponzi scheme) (citing *United States v. Marceau*, 554 F.3d 24, 33 (1st Cir.2009)). *See also United States v. Munyenyezi*, 781 F.3d 532, 545 (rejecting claim that disparity refers to disparity among sentences within a district; finding that 18 U.S.C. § 3553(a)(6) “primarily refers to national disparities among similarly situated defendants.”)

Within this District, conspiracy to commit wire fraud cases are not novel. However, the backdrop of the COVID-19 crisis in the United States is unique. Although other cases involving UI fraud during the COVID-19 pandemic have proceeded to sentencing in this District, none of those cases came close to approaching the magnitude and sophistication of the fraud committed by this group of defendants has been sentenced in this District. In a review across the country as to how various districts have sentenced COVID-19 related fraud cases committed during a time of national crisis, several cases are consistent with the Government's recommendation here and have yielded significant sentences. *See, e.g., United States v. Jerry Phillips*, TDC-22-073 (D. Maryland 2023), the defendant and his co-defendant, Jaleel Phillips,⁶ was sentenced to 84 months (60 months

⁶ The Government notes that defendant Jerry Phillips had a machine gun in his possession at the time of his arrest, which he had purchased as a “ghost gun” and modified.

+ 24 months) for fraud involving pandemic UI benefits, CARES Act Paycheck Protection Program (PPP) loan applications, and Economic Injury Disaster loan (EIDL) applications); *United States v. Kenny Lee Howard*, 24-cr-20142-LVP-DRG, (EDMI, March 13, 2025) (sentenced to 94 months wire fraud and aggravated identity theft for role in COVID-19 UI fraud with \$6.2 million loss (actual), and in excess of \$11 possible); *United States v. Heather Huffman*, 22-cr-00008-JAG-MRC, (E.D. Va. 2024) (former federal employee sentenced to 216 months for wire fraud and aggravated identity theft in COVID-19 UI fraud with \$3.5 million attempted loss and \$2 million actual loss); *United States v. Beaty*, No. 23-2060, 2024 WL 5003232 (6th Cir. December 6, 2024) (affirming W.D.M.I. sentence; defendant sentenced to 124 months (84 months for conspiracy to commit wire fraud + 24 months for aggravated identity theft) for UI (\$760K) and SBA loan fraud (\$300K)); *United States v. Gladstone Njokem*, RDB-21-338 (D. Maryland 2023) (sentencing defendant to 54 months for conspiracy to commit wire fraud and aggravated identity theft for \$1.3M UI fraud with 183 PII victims); *United States v. Eric Michael Jaklitsch*, 22-cr-00015-WBS-1 (EDCA) (sentenced to 81 months (57 months + 24 months) for \$7.5 million UI and Economic Injury Disaster Loan (EIDL) fraud); *United States v. Joseph Marsell Cartlidge, Eric Alexander McMiller, and David Christopher Redfern*, 1:20-CR-340 (M.D.N.C. 2022) (receiving 72 months, 66 months, and 60 months of imprisonment, respectively for submitting fraudulent PPP and EIDL applications, obtaining \$1.2M in loans); *United States v. Lola Kasali*, 4:20-MJ-1106 (S.D. Tex. 2022) (receiving 70 months of imprisonment for submitting two fraudulent PPP loan applications and obtaining \$1.9M in loans); *United States v. Tarik Freitekh*, 3:20-CR-00435 (W.D.N.C. 2022) (receiving 87 months of imprisonment for submitting fraudulent PPP applications and obtaining \$1.75M in loans); *United States v. Adam D. Arena*, 21-MJ-05134 (W.D.N.Y. 2022) (receiving 66

months of imprisonment for his role in fraudulently obtaining and laundering approximately \$950,000 in pandemic loans).

C. Need to Protect the Public (18 U.S.C. § 3553(a)(2)(C))

When fashioning an appropriate sentence, the Court must also consider protecting the public from further crimes committed by the defendant. 18 U.S.C. § 3553(a)(2). A low-end Guideline sentence on Count 2, followed by the consecutive, mandatory 24-month term for Count 7, will protect the public from future crimes of the defendant and will promote respect for the law.

III. CONCLUSION

For all of these reasons, the Government urges this Court to impose the recommended sentence.

Respectfully submitted,

SARA MIRON BLOOM
ACTING UNITED STATES ATTORNEY



DENISE M. BARTON
STACEY A. ERICKSON
Assistant U.S. Attorneys
JOHN MOREIRA
Special Assistant U.S. Attorney
United States Attorney's Office
One Financial Plaza, 17th Floor
Providence, RI 02903
401-709-5000 (office)

CERTIFICATE OF SERVICE

I hereby certify that on this 16 day of March 2025, I caused the within Government's Sentencing Memorandum to be filed electronically and to be available for downloading on the Court's ECF system:

A handwritten signature in blue ink that reads "Denise M. Barton". The signature is written in a cursive, flowing style.

DENISE M. BARTON
Assistant U. S. Attorney,
U. S. Attorney's Office
One Financial Center Plaza, 17th Floor
Providence, RI 02903
401-709-5000

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

UNITED STATES OF AMERICA

CR. No.: 20-CR-0020-MRD

v.

JAMES LEGERME,
Defendant.

GOVERNMENT’S SENTENCING MEMORANDUM

In accordance with the plea agreement, and for the reasons set forth herein, the Government asks the Court to impose a low-end Guideline sentence of imprisonment¹ of 121 months for Defendant James Legerme (Legerme); enter an order of restitution for \$4,456,927.36; and grant the Motion for Preliminary Order of Forfeiture, of specified assets, and the Order of Forfeiture (Money Judgment) in the amount of \$1,214,294.75,² as agreed to by the Defendant in his Plea Agreement. With his co-conspirators, the Defendant engaged in a carefully orchestrated fraud and identify theft scheme, that targeted relief designed to aid those in need during the COVID-19 pandemic, and stole at least \$4.8 million.

¹ The Presentence Report currently calculates the Guideline range as 97-121 months for Count 2 (Conspiracy to Commit Wire Fraud), plus a consecutive 24 months for Count 12 (Aggravated Identity Theft), for a combined Guideline range of 121 – 145 months. ECF 176, Presentence Report, ¶ 106 The Defendant has objected to the application of a +2 enhancement under U.S.S.G. § 3B1.1(c) (Aggravating Role Adjustment), and the lack of a 2 point reduction under U.S.S.G. § 4C1.1 (the Zero Point Offender provisions). The Probation Department has responded that the enhancement is appropriate, and the Government agrees for the reasons set forth herein. However, if the Defendant’s objections are sustained, the Guideline range may change. If the Guideline range changes, the Government will amend its sentencing recommendation at the Sentencing Hearing, to make the agreed-upon low-end Guideline recommendation.

² As set forth in ECF 168, in the *Government’s Motion For (1) Preliminary Order Of Forfeiture And (2) Order Of Forfeiture (Money Judgment)*, in this Plea Agreement, the Defendant agreed to forfeiture of specified assets and that an amount of \$4,857,191 constitutes proceeds of the conspiracy charged in Count 2, and that that he will forfeit a sum of money in the amount of \$1,214,294.75 in the form of a forfeiture money judgement.

I. OUTSTANDING OBJECTIONS

In considering objections and determining what guideline adjustments apply, the Court must find that the Government has made a showing of any fact necessary and relevant to sentencing by a preponderance of the evidence. *United States v. Flete-Garcia*, 925 F.3d 17, 28 (1st Cir. 2019). The Court has “considerable discretion” in determining what evidence should be regarded as reliable for such fact-finding. *Id.* at 28. Because at the sentencing phase a defendant has no right to confront witnesses against him and sentencing courts may rely on hearsay evidence, *see United States v. Rodriguez*, 336 F.3d 67, 71 (1st Cir. 2003), the Court may appropriately rely on documentary information such as the PSR, affidavits, exhibits, and submissions of counsel. *United States v. Curran*, 525 F.3d 74, 78 (1st Cir. 2008) (quoting *United States v. Ranney*, 298 F.3d 74, 81 (1st Cir.2002)). The Court may “evaluate virtually *any* dependable information” to determine the probative value of such information with respect to issues material to sentencing. *United States v. Bradley*, 917 F.2d 601, 605 (1st Cir. 1990) (emphasis added); *see, e.g., United States v. Acevedo-Lopez*, 873 F.3d 330, 340 (1st Cir. 2017) (relying upon hearsay proffer of the AUSA).

The Court may consider relevant information without regard to its admissibility under the rules of evidence applicable at trial, provided that the information has sufficient indicia of reliability, U.S.S.G. § 6A1.3(a), including out-of-court statements by witnesses. *United States v. Lee*, 892 F.3d 488, 492 (1st Cir. 2018). Such indicia may include details, internal consistence, and corroboration by multiple witnesses. *United States v. Green*, 426 F.3d 64, 67 (1st Cir. 2005) (emphasis added).

Evaluation of the submitted information need not involve a hearing. Rather, “[a]t sentencing, evidentiary hearings are the exception, not the rule.” *Flete-Garcia*, 925 F.3d at 34 (citing *United States v. Shattuck*, 961 F.2d 1012, 1014-15 (1st Cir. 1992)). The parties need only

have an “adequate opportunity to present information to the court” about any sentencing factor that is “reasonably in dispute.” *Id.* at 35; U.S.S.G. § 6A1.3(a). Where the Government provides documentary support sufficient for factual findings, there is no need to “bolster” the evidence by calling a live witness. *See United States v. Gerante*, 891 F.2d 364, 367 (1st Cir. 1989).

A. Objection to +2 Under U.S.S.G. § 3B1.1(c)

Defendant Legerme has objected to the +2 adjustment for his role in the offense under U.S.S.G. § 3B1.1(c). *See* Objection to Presentence Report (PSR) (Legerme) and ECF 176-1 PSR. In sum, Legerme claims that he never exercised control over the identified person, Luckson Loussaint (Louissaint); that their relationship is a familial one; and that because Louissaint was not indicted in the case and the case against him was dismissed, he cannot be a “criminally responsible person.” The Defendant’s argument fails on all grounds, as explained below and by the Probation Officer in his Response to the Objection.³ The

U.S.S.G. § 3B1.1 established a tiered approach for aggravating role enhancements. For criminal activity that involved 5 or more participants, or “was otherwise extensive,” a +4 enhancement applies for a defendant who was an organizer or leader, and a +3 enhancement applies for a defendant who was a manager or supervisor. U.S.S.G. § 3B1.1(a) and (b), & Application Note 2. For a defendant involved in other criminal activity that did not involve 5 or more participants or that was not “otherwise extensive,” and who was an organizer, leader, manager, or supervisor” of one or more participant, a +2 enhancement applies. U.S.S.G. § 3B1.1(c), & Application Note 2.

For a U.S.S.G. § 3B1.1(a) and (b) role adjustment to apply, the Government must show *first*, the scope of the criminal activity, specifically that it involved 5 or more participants, or was

³ The Government incorporates the Response to this Objection by the Probation Officer in ECF 176-3, as if set forth fully herein.

otherwise extensive, and *second*, a defendant's status in the criminal activity. *See United States v. Figaro-Benjamin*, 100 F.4th 294, 306-08 (1st Cir. 2024); *United States v. Coplin-Benjamin*, 79 F.4th 36 (1st Cir. 2023).

To assess the numerosity aspect of the scope of criminal activity, the Guidelines provide that a "participant" is a person who is criminally responsible for the commission of the offense, but need not have been convicted." U.S.S.G. § 3B1.1, Application Note 1).

To be considered a participant, it is only necessary that an individual gives knowing aid in some aspect of the criminal activity. Similarly, an individual can be considered a participant when his or her acts "give rise to an inference of complicity sufficient to ground a finding that [the individual] was a participant in the criminal activities."

United States v. Acevedo-López, 873 F.3d 330, 336-37 (2017) (affirming § 3B1.1(a) enhancement). *See also United States v. Tavares*, 705 F.3d 4, 30 (2013) (holding that an immunized witness who was part of the criminal activity may be a "participant"). Further,

[w]ho is considered a member of the conspiracy for purposes of the numerosity criterion is to be broadly construed, and all persons involved in the conspiracy—including outsiders—can be counted towards considering the conspiracy "extensive." *See id.* (quoting USSG § 3B1.1 cmt. 3). Courts may look beyond the number of participants to evaluate whether a conspiracy was "extensive" by considering "the totality of the circumstances, including ... the width, breadth, scope, complexity, and duration of the scheme."

United States v. Goodwin, 617 Fed. Appx. 12, 15 (1st Cir. 2015).

For a U.S.S.G. § 3B1.1(c) role adjustment, the court must determine that a defendant was involved in criminal activity involving at least two participants, one of whom can be the defendant himself, and make a determination as to the defendant's status. *See United States v. Grullon*, 996 F.3d 21, 34-35 (1st Cir. 2021) (citation omitted) (affirming application of +2 U.S.S.G. 3B1.1(c) enhancement; holding "[e]vidence of the defendant's role in the conspiracy . . . need only show that he exercised authority or control over [one other] participant on one occasion."); *United States*

v. Prange, 771 F.3d 17, 34 (2014) (“To justify the two-level enhancement [under § 3B1.1(c)], “[e]vidence of the defendant’s role ... need only show that he ‘exercised authority or control over another *participant* on one occasion.’ ”) (emphasis added); *United States v. Savarese*, 686 F.3d 1, 19 (1st Cir. 2012) (§ 3B1.1(c) applies “if the underlying criminal activity involved at least two, but fewer than five complicit individuals (including the defendant), and the defendant, in committing the offense, . . . exercised control over, managed, organized, or superintended the activities of at least one other *participant*.”) (emphasis added) (citations and quotations omitted)

Application Note 4 of U.S.S.G. 3B1.1 states that:

In making the determination of whether someone is an “organizer or leader” or merely a “manager or supervisor,” courts should consider “the exercise of decision making authority, the nature of participation in the commission of the offense, the recruitment of accomplices, the claimed right to a larger share of the fruits of the crime, the degree of participation in planning or organizing the offense, the nature and scope of the illegal activity, and the degree of control and authority exercised over others.”

However, the First Circuit has cautioned that the list of factors in Application Note 4 “is representative rather than exhaustive, and proof of each and every factor is not necessary to establish that a defendant acted as an organizer or leader.” *See United States v. Coplin-Benjamin*, 79 F.4th at 41 (citations omitted).

With any of the U.S.S.G. § 3B1.1 aggravating role adjustments, a formal, hierarchy or chain of command is not required. *United States v. Figaro-Benjamin*, 100 F.4th at 306-08. Further, multiple persons can serve leadership roles. “[T]he existence of another leader -- even one superior to [defendant] in the scheme’s hierarchy -- does not foreclose the possibility of [defendant] also acting as a leader.” *United States v. Coplin-Benjamin*, 79 F.4th at 42.

The First Circuit has held that it is “a relatively low bar” to show that a defendant exercised some control over another criminal actor. *United States v. Figaro-Benjamin*, 100 F.4th at 307. In

fact, the supervisory authority may be minimal and may have been exercised on a single occasion for a § 3B1.1 enhancement to apply. *Id.* at 307 (finding that defendant’s “role involved at least a minimal degree of control over others, on at least one occasion; defendant’s text messages that showed that he sent a taxi to transport two participants to assist with criminal activity, as well as text messages in which he advised other participants of a date for activity and questioning when another participant didn’t respond promptly.) If a defendant takes a role in recruiting at least one person to aid in the conspiracy, that can be sufficient for the a managerial-role enhancement. *See United States v. Savarese*, 686 F.3d at 19-20 (affirming application of U.S.S.G. 3B1.1(c) enhancement). In *Savarese*, the Court rejected the defendant’s claim that the enhancement didn’t apply because he didn’t hold any supervisory role, and found that his role in recruiting another was sufficient.

That “[Defendant] was by no means the mastermind of the operation, that is not the standard by which “managerial” status is governed. A defendant’s exhibitions of authority need be neither supreme nor continuous; we have even held that, in some circumstances, the government need only show by a preponderance of the evidence “that the defendant exercised authority or control over another participant on one occasion.”

Id. at 20 (citation omitted). See also *United States v. Prange*, 771 F.3d at 35 (affirming application of U.S.S.G. 3B1.1(c) enhancement, finding that “at a minimum, [defendant] recruited Jordan and multiple other executives into this scheme by introducing them to E.H., gauging their willingness to issue kickbacks, and recommending them to the agent.”)

In this case, Defendant Legerme recruited his cousin, Luckson Louissaint, to aid him and his co-conspirators, and thereafter oversaw, supervised, and managed Louissaint’s efforts that aided Legerme and his co-defendants. At Legerme’s direction, Louissaint created email addresses for his co-conspirators and used his address to receive fraudulent debit cards, which were later sent to Legerme. When interviewed by law enforcement, Louissaint admitted that he made email

addresses for Legerme, and that he sent them to him.⁴ Text messages between Legerme and Louissaint show communications relating to Louissaint's efforts for Legerme, as well as for "T" [Tony MERTILE]; "P" [Junior "Peanut" MERTILE]; "G," "Fat Ass," [uncharged co-conspirator Pierre Cadet]. *See* Exhibit 1, Text Messages Between Legerme and Louissaint. Additional information showing Louissaint's connection to Legerme and his co-conspirators, and Legerme's supervision, leadership, and/or management of Louissaint are set forth in the attached Affidavit, that was submitted in support of a complaint charged Louissaint. *See* Exhibit 12, Complaint and Affidavit, Case No. 1:21MJ59LDA, *United States v. Louissaint*. The fact that the charges were ultimately dismissed against Louissaint does not undercut the fact that ample facts exists to show by a preponderance that a U.S.S.G. 3B1.1 enhancement is warranted for Legerme's actions with his cousin, Luckson Louissaint.

B. Objection as to Zero Point Offender

In addition to his objection on the U.S.S.G. § 3B1.1(c) enhancement, the Defendant objects to lack of a 2 point reduction under U.S.S.G. § 4C1.1, the Zero Point Offender provision. In relevant part, U.S.S.G. § 4C1.1 provides that:

If the defendant meets all of the following criteria:

- (1) the defendant did not receive any criminal history points from Chapter Four, Part A;

⁴ Although Louissaint claimed that he made the email addresses for Legerme's Air BnB business, that explanation was not credible. *See* Complaint Affidavit, Exhibit 2, ¶ 32 ("LOUISSAINT also claimed that he did make email addresses for Legerme, but it was for Legerme to use to give his business and AirBNBs good reviews. LOUISSAINT claimed he made 20 emails at one time and 20 or 30 email addresses another time. According to records from AirBNB, Legerme is not an AirBNB host. Legerme's wife, Shemka Williams is a host of one AirBNB property in Fort Lauderdale, FL. However, AirBNB records show that there are only 13 reviews for that property, and the last five reviews were March 1, March 11, March 15, March 21, and April 3, 2020. I note that LOUISSAINT's and Legerme's messages described above occurred between March 22, 2020 and June 6, 2020.")

(10) the defendant did not receive an adjustment under §3B1.1 (Aggravating Role); and

decrease the offense level determined under Chapters Two and Three by 2 levels.

U.S.S.G. § 4C1.1. The Defendant's role in the conspiracy, and consequent role adjustment under U.S.S.G. § 3B1.1(c), makes him ineligible for a reduction under U.S.S.G. § 4C1.1.

II. SENTENCING RECOMMENDATION

The sentence recommended by the Government is a significant, and a "sufficient but not greater than necessary" sentence, taking into account all of the 18 U.S.C. § 3553(a) sentencing factors, the Congressional mandate that the sentence for Aggravated Identity Theft, 18 U.S.C. § 1028A, and case law re 1028A.

A. Defendant's Conspiracy to Commit Wire Fraud Sentence Cannot Be Reduced or Lessened Due to 24 Month Sentence to be Imposed for Aggravated Identify Theft.

As a preliminary matter, the Defendant stands before the Court convicted of Conspiracy to Commit Wire Fraud and Aggravated Identity Theft. The sentence for his Aggravated Identity Theft conviction must, by statute, be 24 months consecutive to whatever sentence the Court imposes for his conviction for Conspiracy to Commit Wire Fraud.

As this Court is aware, in accordance with the penalty provision of 18 U.S.C. § 1028A and the case law interpreting that statute, a sentencing court must determine the sentence for Count 2, Conspiracy to Commit Wire Fraud, the predicate offense in this case, independent of, and without regard for, the mandatory minimum sentence to be imposed for his violation of Count 12, Aggravated Identify Theft, and may not discount or offset the conviction for the predicate offense due to the mandatory minimum sentence to be imposed. 18 U.S.C. § 1028A(b)(3) states that:

in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or

otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

18 U.S.C. § 1028(b)(3) (emphasis added).

The Supreme Court, First Circuit, and other Circuits have consistently recognized that a sentencing court cannot reduce or offset the sentence to be imposed on a predicate offense due to the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A. In *Dean v. United States*, the Court held that 18 U.S.C. § 924(c), another statute setting a consecutive, mandatory minimum, did not prohibit consideration of the mandatory minimum sentence when determining sentence on the predicate offense. However, the Court expressly recognized the difference in the statutory language of 18 U.S.C. § 1028A and 18 U.S.C. § 924(c), and found that 18 U.S.C. § 1028A did not afford sentencing courts the same discretion as courts had under 18 U.S.C. § 924(c).

Congress has shown just that in another statute, 18 U.S.C. § 1028A. That section, which criminalizes the commission of identity theft “during and in relation to” certain predicate felonies, imposes a mandatory minimum sentence “in addition to the punishment provided for” the underlying offense. § 1028A(a)(1). It also says that the mandatory minimum must be consecutive to the sentence for the underlying offense. § 1028A(b)(2). So far, § 1028A tracks § 924(c) in relevant respects. But § 1028A goes further: It provides that in determining the appropriate length of imprisonment for the predicate felony “a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section.” § 1028A(b)(3).

Dean vs. United States, 581 U.S. 62, 70 (2017). The First Circuit has also recognized this statutory mandate, finding that a sentencing court may not consider the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A, when determining the sentence for enumerated predicate offenses, such as Conspiracy to Commit Wire Fraud. *See United States v. Vidal-Reyes*, 562 F.3d 43, 54 (1st Cir. 2009) (holding that sentencing courts has authority to consider the § 1028A mandatory minimum sentence when determining sentences for non-predicate offenses, but not for

predicate offenses). As the First Circuit observed, “a major concern of § 1028A(b)(3)’s drafters was to ensure, by making the sentences truly cumulative, that prosecutors had an incentive to charge both the aggravated identity theft violation and the underlying predicate felony or felonies.” *Id.* (construing H.R.Rep. No. 108-528, at 10, to show that the bill amended Title 18 to provide for a “mandatory consecutive penalty enhancement of 2 years for any individual who knowingly transfers ... the means of identification of another person in order to commit a serious Federal predicate offense”). Other Circuits have held the same. The Third Circuit has held that:

There is no doubt that § 1028A(b)(3) “bar[s] consideration of a mandatory minimum” during sentencing for the predicate felony.⁹ The Supreme Court as well as the First, Seventh, Eighth, Ninth, and Tenth Circuits have explained that under § 1028A, a sentencing court cannot reduce the sentence it would have otherwise imposed on a predicate conviction because of the knowledge of a defendant’s two-year mandatory minimum sentence for aggravated identity theft.

United States v. Yusuf, 781 Fed. Appx. 77, 80 (3rd Cir. 2019) (unpublished) (vacating sentencing and remanding; finding that the district court improperly considered the mandatory minimum sentence to be imposed under 18 U.S.C. § 1028A when imposing sentence on the predicate offense). Similarly, the Tenth Circuit found that:

Indeed, we indicated in [*United States v. Smith*, 756 F.3d 1179, 1185–87 (10th Cir. 2014)] that § 1028A(b)(3)’s plain language “does” precisely “what it says”: it “prevent[s] a sentencing court from taking account of § 1028A[(a)(1)]’s mandatory minimum[] when considering a sentence for predicate offenses” such as bank fraud. And we noted in *Smith* that our sister circuits have reached the same conclusion. . . . Thus, we hold that § 1028A(b)(3) prohibited the district court *437 from considering § 1028A(a)(1)’s two-year sentence for aggravated identify theft in crafting Lara’s sentences for bank fraud.

United States v. Lara, 733 Fed. Appx. 433 (10th Cir. 2018) (unpublished) (same) (collecting cases).

A. Nature and Circumstances of the Offense (18 U.S.C. § 3553(a)(1))

The “nature and circumstances of the offense” are egregious and compelling and warrant a significant, lengthy period of incarceration.

For most Americans, the COVID-19 pandemic resulted in an unprecedented time of financial hardship, turmoil, and suffering, but for the Defendant and his conspirators, it constituted a lucrative opportunity to enrich themselves with funds intended for unemployed workers. While most individuals were sheltering in place, taking care of loved ones, and often making tough financial sacrifices, the Defendant and his co-conspirators collaborated amongst themselves, and with others, to take advantage of programs meant to help those in need and did so for their own selfish purposes. The Defendant’s conduct victimized numerous government entities, and countless individuals, whose personal identifying information (PII) was used by the Defendant and his co-defendants.

As the pandemic ravaged the country, Congress appropriated billions of dollars to create or supplement government relief programs. Because this assistance was desperately needed by unemployed workers, independent contractors, nonprofits, and small businesses for their survival, the government made a policy decision to deliver the relief on an unprecedented scale as quickly as possible. In the spring of 2020, Congress passed the Coronavirus Aid, Relief and Economic Security (CARES) Act, which provided for a variety of economic benefits to struggling Americans during a time of severe negative economic impact as a result of the COVID-19 pandemic. At the time, the federal government had taken several steps to mitigate the effects of the pandemic on businesses and workers. The Families First Coronavirus Response Act (FFCRA) and Coronavirus Aid, Relief, and Economic Security (CARES) Act provided additional funding to assist workers who were unemployed/had hours cut as a direct result of the COVID-19 pandemic. The money

was distributed to the state workforce agencies (SWAs) which handled the disbursement of traditional (state) Unemployment Insurance (UI) benefits, and the SWA disbursed the additional federal benefits. The CARES Act allowed states to expand the scope of workers who were eligible to receive state UI benefits, to extend the period of time for which workers could be eligible for UI benefits, and to allow workers who may have exhausted UI benefits under traditional programs to receive benefits. The CARES Act further expanded the ability of states to provide benefits to unemployed workers by creating three new unemployment programs, namely, the Pandemic Unemployment Assistance (PUA) program, which permitted states to provide benefits to individuals who were self-employed, seeking part-time employment, or otherwise would not qualify for regular unemployment benefits; the Federal Pandemic Unemployment Compensation (FPUC) program, which provided an additional benefit, initially in the amount of \$600 and later, in the amount of \$300, in federal benefits to individuals collecting traditional UI program benefits or PUA benefits; and the Pandemic Emergency Unemployment Compensation (PEUC) program, which provided additional weeks of benefits for individuals who had otherwise exhausted their entitlement to regular UI benefits (collectively referred to herein as “expanded pandemic UI benefits”). This legislation was much needed, as millions of unemployed workers across the United States turned to the unemployment insurance program as their jobs were imperiled by the effects of the pandemic.

It was within this backdrop that the conspirators concocted and executed a scheme to unjustly divert finite unemployment insurance benefits from unemployed workers to themselves. Exploiting vulnerabilities in the execution of this massive relief effort, the defendant and his conspirators devised and repeatedly executed a fraud scheme targeting COVID-19 reliefs,

including the Pandemic Unemployment Assistance Program. Specifically, the Defendant and his conspirators:

- obtained through various means the PII, including dates of birth and Social Security numbers, of identity theft victims;
- in preparation of submitting fraudulent applications to various state workforce agencies for unemployment benefits, the conspirators created and maintained email accounts to facilitate communications with state workforce agencies in the names of those for whom the conspirators had obtained PII;
- filed materially false and misleading unemployment applications with multiple state workforce agencies using the PII of identity theft victims in their possession, and on these applications, the conspirators provided fabricated employment and wage history, along with false contact information, such as physical and mailing addresses, email addresses, and phone numbers that did not, in fact, belong to the purported applicant;
- falsely certified the truth and accuracy of all the information included in the aforementioned applications, such as the purported applicants' eligibility to receive the benefits when, in truth and in fact, the conspirators then and there well knew that the information was not true and accurate, the purported claimants were not eligible for the requested benefits, and those benefits were actually being paid to conspirators and not the purported claimants;
- opened and created bank accounts using the PII of identity theft victims, and obtained debit cards for those bank accounts, and directed the state workforce agencies to directly deposit the benefit payments to the bank accounts in the names of others and/or in bank accounts controlled by them;
- once their fraudulent applications were approved, the conspirators kept, maintained, and shared amongst themselves possession of the prepaid debit cards loaded with benefit payments, and the conspirators distributed the fraud proceeds amongst themselves and others; and
- for many of the approved applications, the conspirators would often double down on, and repeat their fraud by submitting weekly recertifications of unemployment status to the state workforce agencies, falsely claiming that the purported claimant was still unemployed and entitled to receive additional unemployment benefits.

Given the scope of and means by which the Defendant and his co-conspirators committed this massive fraud, the Government was unable to fully identify the full amount of actual and attempted losses. However, the Government was able to determine, through analysis of bank records, and the parties have agreed to a loss amount of \$4,857,191, which is based on the actual loss amount determined from review of a myriad of bank records. Therefore, the Defendant stands before this Court for being part of a conspiracy that stole nearly \$5 million.

As laid out above and in the PSR, the conspirators' scheme was labor intensive, sophisticated, and multifaceted – recruiting co-conspirators and other participants to aid in their enormous fraud, obtaining PII through various means, maintaining and distributing the PII information amongst members of the conspiracy, preparing and submitting fraudulent applications for hundreds of purported claimants, recertifying fraudulent applications on a weekly basis, creating and maintaining email accounts to facilitate communications with the state workforce agencies, forging and falsifying documents to substantiate the false information provided in the fraudulent applications, and maintaining and distributing prepaid debit cards and the fraud proceeds amongst the members of the conspiracy. The repetitive, continuous nature of the fraud makes clear that the conspirators' criminal conduct was not a product of a momentary lapse of judgment; instead, it was a rational, deliberate choice that the conspirators knowingly and willfully made over and over again. The volume, duration, and scope of the conspirators' scheme is staggering and indicative of the greed motivating the conspirators' criminal conduct.

By looting the unemployment program, the conspirators repeatedly stole finite funds from those who needed it the most during the pandemic, and their relentless pursuit of these funds showed a callous disregard to unemployed workers, identity theft victims, state workforce agencies – who had the daunting task of administering an unprecedented relief effort – and American

taxpayers, whose earnings underlie the funds in question. Through their criminal conduct, the conspirators interfered with and undermined the federal government's efforts to provide necessary and urgent relief to Americans harmed by the pandemic. The nature and circumstances of the offense well support a substantial sentence for each conspirator.

During search warrants executed at the homes of the 4 co-Defendants, investigators recovered a total of 994 debit cards from multiple banks, shown below, most of which were in the names of third parties and had been used to obtain fraudulent expanded pandemic UI benefits. The evidence recovered from the Defendant's home, as well as review of bank records for accounts associated with the Defendant (fraudulently opened accounts and accounts in their names) show that Defendant Legerme, and his co-conspirators, had been using fraudulently obtained PII to obtain fraudulent payment from multiple federal and state government agencies prior to the pandemic. As a result, the when the COVID-19 pandemic began, the Defendants used their knowledge, and established systems, to defraud the Government programs to aid those struggling with COVID-19 pandemic.⁵

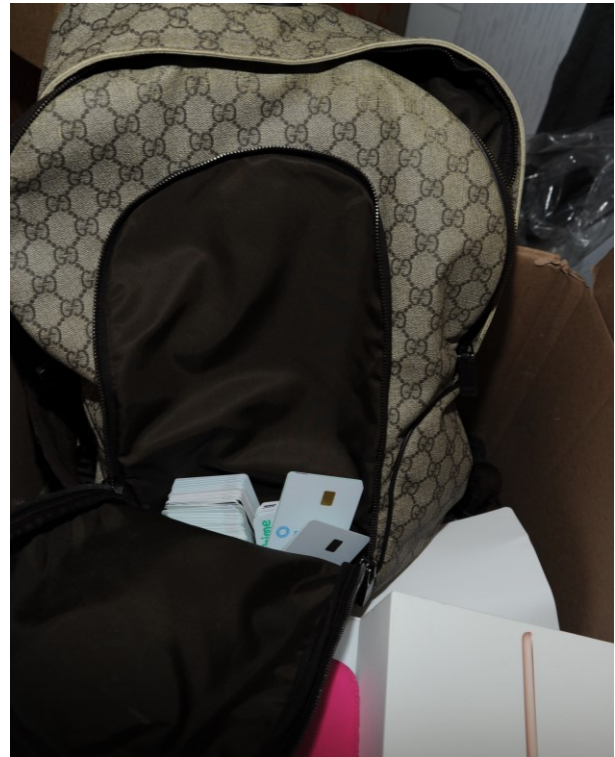
⁵ In their Plea Agreements, each of the Defendants have agreed to engaging in activity "beginning on an unknown date, but not later than January 2019 and continuing through on or about October 13, 2020," which was the date of the arrests of J Legerme, T. Mertile, and J. Mertile. See Plea Agreements, ¶ 4a.

BANK	# OF CARDS
Chime	175
GoBank	295
Green Dot	229
Bank of America	61
Wells Fargo	94
Sun Trust	16
Bancorp	34
Metabank	9
BBVA	8
AMEX	23
PNC	6
Chase	6
Sutton Bank	13
Comerica	20

Lili-Choice Financial Group	1
KeyBank	1
Venmo	
Republic Bank & Trust	1
U.S. Bank	1
Navy Federal CU	1
TOTAL CARDS SEIZED	994

Although the search of co-defendant Tony Mertile's residence resulted in the seizure of the largest amount of currency and debit cards, as shown below, from Defendant Legerme's residence, agents seized approximately \$27,738,000 in cash, as well as numerous debit cards and multiple flip phones. PSR, ¶ 32. In addition, during execution of Legerme's home, a PNC debit card in the name of a victim of identity theft, R.S. was found at the home of James LEGERME; that card was used to purchase access to accounts with Been Verified and Intelius. For example, the following accounts were created: Intelius LLC / People Connect (in the name of Allen Bien-Aime) created on December 31, 2018; from Intelius LLC / People Connect (in the name of R.S. created on 8/30/2019), and Been Verified (in the name of R.S. created on August 30, 2019). PSR, ¶ 36.

Recovered from Residence of James Legerme







The Government further notes that Defendant Legerme was observed in numerous ATM surveillance videos withdrawing funds from fraudulent cards, of which one image is shown below. The hat Legerme is wearing in this image was found in his vehicle when search warrants were executed at his home and vehicle.





Recovered from the Residence of Tony Mertile

- Approximately \$858K cash seized



DRAFT

10





B. History and Characteristics of the Defendant (18 U.S.C. § 3553(a)(1))

Defendant Legerme has no criminal history. However, he has engaged in fraudulent activity using fraudulently obtained PII and fraud on the government before. He was arrested in 2013 in North Miami Beach, and found in possession of Chase and Western Union cards in the names of other persons. Legerme admitted to filing fraudulent tax returns; and said that one of his

“homeboys” taught him how to do tax fraud. PSR, ¶ 45. He was not convicted for that conduct, and appears to have continued with his fraud involving false identities.

C. Need to Afford General and Specific Deterrence (18 U.S.C. § 3553(a)(2)(B))

Under 18 U.S.C. § 3553(a)(2)(B), there is a need “to afford adequate deterrence to criminal conduct.” A significant sanction needs to be imposed to send a signal to others who would contemplate engaging in wire fraud and aggravated identity theft, and to this Defendant to never return to this type of criminal activity. In this respect, the Government submits that a low-end Guideline sentence on Count 2, followed by the consecutive, mandatory 24-month term for Count 12 is justified in this case.

General deterrence is particularly important sentencing factor in fraud cases such as this one because it is viewed to be effective. The deliberate nature of fraud often renders it more difficult to uncover, since individuals engaged in fraud take affirmative steps to conceal their identities and conduct. The First Circuit, among others, has “emphasized the importance of general deterrence of white collar crime.” *United States v. Prosperi*, 686 F.3d 32, 47 (1st Cir. 2012); *see also United States v. Mueffelman*, 470 F.3d 33, 40 (1st Cir. 2006) (stating that “the deterrence of white collar crime” was “of central concern to Congress”); *also United States v. Landry*, 631 F.3d 597, 607 (affirming wire fraud and aggravated identify theft sentence; finding that the district court did not err in considering the need for the sentence to afford deterrence in an aggravated identity theft case); *United States v. Martin*, 455 F.3d 1227, 1240 (11th Cir. 2006) (“Because economic and fraud-based crimes are ‘more rational, cool, and calculated than sudden crimes of passion or opportunity’ these crimes are ‘prime candidates for general deterrence.’ ” *quoting* Stephanos Bibas, White-Collar Plea Bargaining and Sentencing After Booker, 47 Wm. & Mary L. Rev. 721, 724 (2005)).

The COVID-19 pandemic and programs created to aid struggling Americans citizens, residents, and businesses, led to a surge in identity theft and fraud against government programs in 2020 and thereafter, resulting in estimated hundreds of billions of total losses.⁶ Despite its best efforts, law enforcement will not ever be able to identify, catch, and convict all of the opportunistic fraudsters who made off with taxpayers' funds during the pandemic. The case against this Defendant, and his co-conspirators, presents a worthwhile opportunity for the Court to impose a sentence that will grab the attention of those who may be considering similar crimes. The recommended sentence of imprisonment for this fraud scheme is "sufficient, but not greater than necessary" to deter this Defendant, and other who may consider engaging in similar conduct.

D. Need to Reflect the Seriousness of the Crimes, Promote Respect for the Law, and Need to Provide Just Punishment (18 U.S.C. § 3553(a)(2)(C))

The Defendant's crimes are unquestionably serious. During the height of the COVID-19 pandemic, he and his conspirators countlessly executed a fraud scheme targeting state workforce agencies that were administering COVID-19 relief to unemployed workers. The conspirators unjustly diverted at least \$4,857,191 in unemployment benefits from overburdened government agencies and desperate, unemployed workers to themselves. By numbers alone, the criminal conduct is extremely serious, but the harm in this case cannot be measured solely by financial losses. The defendant's criminal conduct imposed other non-pecuniary harms on primary and secondary victims.

First, by flooding state workforce agencies with hundreds upon hundreds of fraudulent unemployment applications, the defendant raised administrative costs for these agencies, likely

⁶ See Richard Lardner et al, The Great Grift: How billions in COVID-19 relief aid was stolen or wasted, Associated Press, June 12, 2023, <https://apnews.com/article/pandemic-covid19-fraud-small-business-inspector-general-7e651b3e405863f0be9f2e34ca47b93e>

delaying the approval of legitimate applications by unemployed workers. This harm is far from theoretical. Facing lengthy delays in the adjudication of unpaid claims, genuinely unemployed workers initiated class action litigation against the VEC during the pandemic in order to obtain unemployment benefits owed to them in a timely manner. As United States District Court Judge Henry E. Hudson aptly observed in the separate class action on this matter, “the unprecedented COVID-19 pandemic and pandemic-related restrictions caused a significant increase in unemployment claims and overwhelmed unemployment compensation programs nationwide, including in Virginia.” *Cox et al. v. Hess*, Case No. 3:21-cv-253-HEH, Dkt. No. 25 at 1 (Order). The defendant’s sentence must reflect the harm to unemployed workers who suffered lengthy delays in the approval of their legitimate unemployment claims and the receipt of much needed benefits due to the increase in administrative costs on state workforce agencies caused by the conspirators’ submission of numerous fraudulent applications.

Second, although the identity theft victims in this case did not directly suffer a financial loss to the Government’s knowledge, being the victim of identity theft is truly a life altering experience, nonetheless. In addition to potential financial harm, many victims of identity theft suffer devastating emotional and psychological trauma from these crimes, resulting in feelings of anger, fear, anxiety, depression, confusion, and more. Moreover, the conspirators filing claims using the PII of identity theft victims potentially hampered the ability of these individuals to obtain unemployment benefits and created potential tax liabilities for victims who never knew of or received the unemployment benefits obtained in their names.

Fourth and finally, while the state workforce agencies and identity theft victims are the ostensible victims in this case, the Defendant and his co-conspirators also defrauded American

taxpayers whose earnings underlie the government program in question. In sum, the Defendant's crimes are serious and deserving of a lengthy term of imprisonment.

C. Need to Avoid Unwarranted Sentencing Disparities (18 U.S.C. § 3553(a)(6))

Under 18 U.S.C. § 3553(a)(6), there is a need to “avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct.” “Section 3553(a)(6) ‘is primarily aimed at national disparities, rather than those between co-defendants.’” *United States v. Reyes-Rivera*, 812 F.3d 79, 90 (1st Cir. 2016) (affirming 242 month sentence for \$22 million Ponzi scheme) (citing *United States v. Marceau*, 554 F.3d 24, 33 (1st Cir.2009)). *See also United States v. Munyenyezi*, 781 F.3d 532, 545 (rejecting claim that disparity refers to disparity among sentences within a district; finding that 18 U.S.C. § 3553(a)(6) “primarily refers to national disparities among similarly situated defendants.”)

Within this District, conspiracy to commit wire fraud cases are not novel. However, the backdrop of the COVID-19 crisis in the United States is unique. Although other cases involving UI fraud during the COVID-19 pandemic have proceeded to sentencing in this District, none of those cases came close to approaching the magnitude and sophistication of the fraud committed by this group of defendants has been sentenced in this District. In a review across the country as to how various districts have sentenced COVID-19 related fraud cases committed during a time of national crisis, several cases are consistent with the Government's recommendation here and have yielded significant sentences. *See, e.g., United States v. Jerry Phillips*, TDC-22-073 (D. Maryland 2023), the defendant and his co-defendant, Jaleel Phillips,⁷ was sentenced to 84 months (60 months + 24 months) for fraud involving pandemic UI benefits, CARES Act Paycheck Protection Program

⁷ The Government notes that defendant Jerry Phillips had a machine gun in his possession at the time of his arrest, which he had purchased as a “ghost gun” and modified.

(PPP) loan applications, and Economic Injury Disaster loan (EIDL) applications); *United States v. Kenny Lee Howard*, 24-cr-20142-LVP-DRG, (EDMI, March 13, 2025) (sentenced to 94 months wire fraud and aggravated identity theft for role in COVID-19 UI fraud with \$6.2 million loss (actual), and in excess of \$11 possible); *United States v. Heather Huffman*, 22-cr-00008-JAG-MRC, (E.D. Va. 2024) (former federal employee sentenced to 216 months for wire fraud and aggravated identity theft in COVID-19 UI fraud with \$3.5 million attempted loss and \$2 million actual loss); *United States v. Beaty*, No. 23-2060, 2024 WL 5003232 (6th Cir. December 6, 2024) (affirming W.D.M.I. sentence; defendant sentenced to 124 months (84 months for conspiracy to commit wire fraud + 24 months for aggravated identity theft) for UI (\$760K) and SBA loan fraud (\$300K)); *United States v. Gladstone Njokem*, RDB-21-338 (D. Maryland 2023) (sentencing defendant to 54 months for conspiracy to commit wire fraud and aggravated identity theft for \$1.3M UI fraud with 183 PII victims); *United States v. Eric Michael Jaklitsch*, 22-cr-00015-WBS-1 (EDCA) (sentenced to 81 months (57 months + 24 months) for \$7.5 million UI and Economic Injury Disaster Loan (EIDL) fraud); *United States v. Joseph Marsell Cartlidge, Eric Alexander McMiller, and David Christopher Redfern*, 1:20-CR-340 (M.D.N.C. 2022) (receiving 72 months, 66 months, and 60 months of imprisonment, respectively for submitting fraudulent PPP and EIDL applications, obtaining \$1.2M in loans); *United States v. Lola Kasali*, 4:20-MJ-1106 (S.D. Tex. 2022) (receiving 70 months of imprisonment for submitting two fraudulent PPP loan applications and obtaining \$1.9M in loans); *United States v. Tarik Freitekh*, 3:20-CR-00435 (W.D.N.C. 2022) (receiving 87 months of imprisonment for submitting fraudulent PPP applications and obtaining \$1.75M in loans); *United States v. Adam D. Arena*, 21-MJ-05134 (W.D.N.Y. 2022) (receiving 66 months of imprisonment for his role in fraudulently obtaining and laundering approximately \$950,000 in pandemic loans).

D. Need to Protect the Public (18 U.S.C. § 3553(a)(2)(C))

When fashioning an appropriate sentence, the Court must also consider protecting the public from further crimes committed by the defendant. 18 U.S.C. § 3553(a)(2). A low-end Guideline sentence on Count 2, followed by the consecutive, mandatory 24-month term for Count 12, will protect the public from future crimes of the defendant and will promote respect for the law.

III. CONCLUSION

For all of these reasons, the Government urges this Court to impose the recommended sentence.

Respectfully submitted,

SARA MIRON BLOOM
ACTING UNITED STATES ATTORNEY

A handwritten signature in blue ink that reads "Denise M. Barton".

DENISE M. BARTON
STACEY A. ERICKSON
Assistant U.S. Attorneys
JOHN MOREIRA
Special Assistant U.S. Attorney
United States Attorney's Office
One Financial Plaza, 17th Floor
Providence, RI 02903
401-709-5000 (office)

CERTIFICATE OF SERVICE

I hereby certify that on this 16 day of March 2025, I caused the within Government's Sentencing Memorandum to be filed electronically and to be available for downloading on the Court's ECF system:

A handwritten signature in blue ink that reads "Denise M. Barton". The signature is written in a cursive, flowing style.

DENISE M. BARTON
Assistant U. S. Attorney,
U. S. Attorney's Office
One Financial Center Plaza, 17th Floor
Providence, RI 02903
401-709-5000

EXHIBIT 1

Son

[Redacted] 68084



Saturday, June 6, 2020

S Yo yo yo ...

Lol 8:39 PM

9:12 PM

S What's up 9:13 PM

9:17 PM Just woke up . What's up

9:24 PM Getting the money now for you

S Ok 10:38 PM

Sunday, June 7, 2020

S You forget me 10:07 PM

10:08 PM Sent

10:09 PM T ,d ,fat and I only use half

S Ok 10:10 PM

10:10 PM Yiu got it ?

S Yah I got it 10:11 PM

Ok



Son

8084

You make gmail and Yahoo too no problem

1:17 AM

S

Ok

6:08 AM

Every 20 send dont wait to have over 100 please sir thank you

3:34 PM

Friday, March 13, 2020

If you have ready send

10:33 AM

Thursday, March 19, 2020

Do more ...

I sent fatass , and T money

10:42 AM

Waiting on G and p

10:43 AM

Friday, March 20, 2020

Need more soon

11:59 AM

S

Ok

12:10 PM

Saturday, March 21, 2020

Let me know when send ...

P/100

G/100

Still owe



Enter message



SEND

Son

8084

1:17 AM

You make gmail and Yahoo too no problem

S

Ok

6:08 AM

3:34 PM

Every 20 send dont wait to have over 100 please sir thank you

Friday, March 13, 2020

10:33 AM

If you have ready send

Thursday, March 19, 2020

Do more ...

10:42 AM

I sent fatass , and T money

10:43 AM

Waiting on G and p

Friday, March 20, 2020

11:59 AM

Need more soon

S

Ok

12:10 PM

Saturday, March 21, 2020

Let me know when send ...

P/100

G/100

Still owe



Enter message



SEND

Son

58084

You make gmail and Yahoo too no problem

1:17 AM

Ok

6:08 AM

Every 20 send dont wait to have over 100 please sir thank you

3:34 PM

Friday, March 13, 2020

If you have ready send

10:33 AM

Thursday, March 19, 2020

Do more ...

I sent fatass , and T money

10:42 AM

Waiting on G and p

10:43 AM

Friday, March 20, 2020

Need more soon

11:59 AM

Ok

12:10 PM

Saturday, March 21, 2020

Let me know when send ...

P/100

G/100

Still owe

Enter message

SEND

Son

8084

Saturday, March 21, 2020

Let me know when send ...

P/100

G/100

Still owe

Everytime you give I will send a
note of balance

10:51 AM

P wanting on you and fat ass

4:50 PM

S

I'm working di la

4:50 PM

Ok lol just making sure

4:50 PM

S

Map voye pita

4:50 PM

You got atleast 20 for p

5:25 PM

You can send 20 now for p

5:32 PM

Let me know when send ...

P/200

G/100

Still owe

5:59 PM

Sunday, March 22, 2020

I'm done with the 20 ... if you



Enter message



SEND

Son

8084

Sunday, March 22, 2020

2:45 AM I'm done with the 20 ... if you have 20 for me go ahead and send 🙏🙏

S Give me 1 more hours 10:39 AM

10:51 AM Ok

S Tcheke Whatsapp Ou 11:39 AM

11:44 AM Ok

11:48 AM I'm not home yet but

Monday, March 23, 2020

2:28 AM P/200
G/100
Fat / 100

S That's all 6:53 AM

7:34 AM I didnt send to everybody yet

Its suppose to be

P/200
G/200
Fat /100
T/100

Enter message

SEND

Son

8084

2:20 AM

S

That's all

6:53 AM

7:34 AM

I didnt send to everybody yet

Its suppose to be

P/200

G/200

Fat /100

T/100

Me/100

7:35 AM

S

Yah

It's ok

7:44 AM

7:46 AM

Hold on

S

Do you have 50\$?

10:55 AM

10:55 AM

I'll send my 100

S

Ok

10:55 AM

11:11 AM

P/200

G/200

T/100

Fat /100

S



12:21 PM



Enter message



SEND

Son

58084

Tuesday, March 24, 2020

P/250 p took 50 from G
G/150
T/100



3:17 PM

Fat paid today

S

Ok cool

3:31 PM

Thursday, March 26, 2020

4:51 PM

Do more



S

100 ?

5:37 PM

5:38 PM

Yes



S



5:38 PM

Friday, March 27, 2020

12:16 PM

I need by Sunday for me .. I'll be
done with everything today ...
so I if you have let me know



12:17 PM

Waiting for
P 250
T 100
G 150
Payment



SEND

Son

8084

S Everything close at 4hr pm

Up noth

North 2:42 PM

S At 5 nobody can't go outside 2:43 PM

2:43 PM Ok sending now

S Ok 2:44 PM

Invoice

2:51 PM T 100

S Ok 2:57 PM

Sunday, March 29, 2020

2:12 PM You'll be done today ?

S [Lebo \[REDACTED\]@aol.com](#)

Happyy05

60

Done 2:21 PM

2:21 PM Ok

Done

Enter message

SEND

Son

58084

2:23 PM

Do more



Old invoice / owe



T 100

New invoice

P 100

Fat 100

Me 100

2:32 PM

Waiting for G and T for new one still have it

S

Ok cool

2:40 PM

Thursday, April 2, 2020

Invoice



T 100

New invoice

P 100

Fat 100

Me 200

2:58 PM

Need more



2:59 PM

Still have 20 left but i'm giving it to t but I need lol so 🙄

Son

8084

Need more

Still have 20 left but i'm giving it
to t but I need lol so 🤔

2:59 PM

S

Ok, 100 more

2:59 PM

S

?

3:00 PM

Yea go ahead

I owe you 200
P owe 100
Fat 100
T 100

3:01 PM

Right now

S

Ok

Sounds great 👍

3:01 PM

If you send more .. I will give it
to everybody and it will be

P 200
Fat 200
T 200
Me 300
G 100

3:02 PM

I don't got it

3:03 PM

I owe you 200



SEND

Enter message

Son

8084

S

Ok, you just don't put the 20 we have down

I got u 😊

3:06 PM

I never paid you for Tony first 20

3:07 PM

S

1100

3:20 PM

Saturday, April 4, 2020

5:02 PM

When you'll be ready ?

S

Tomorrow morning

5:08 PM

5:22 PM

Ok

Sunday, April 5, 2020

6:06 PM

👁️

Monday, April 6, 2020

S

[Emelynw\[REDACTED\]76@aol.com](mailto:Emelynw[REDACTED]76@aol.com)

Happy06

Good night 😴

4:58 AM

7:17 AM

Ok

Ima call you, when she finish

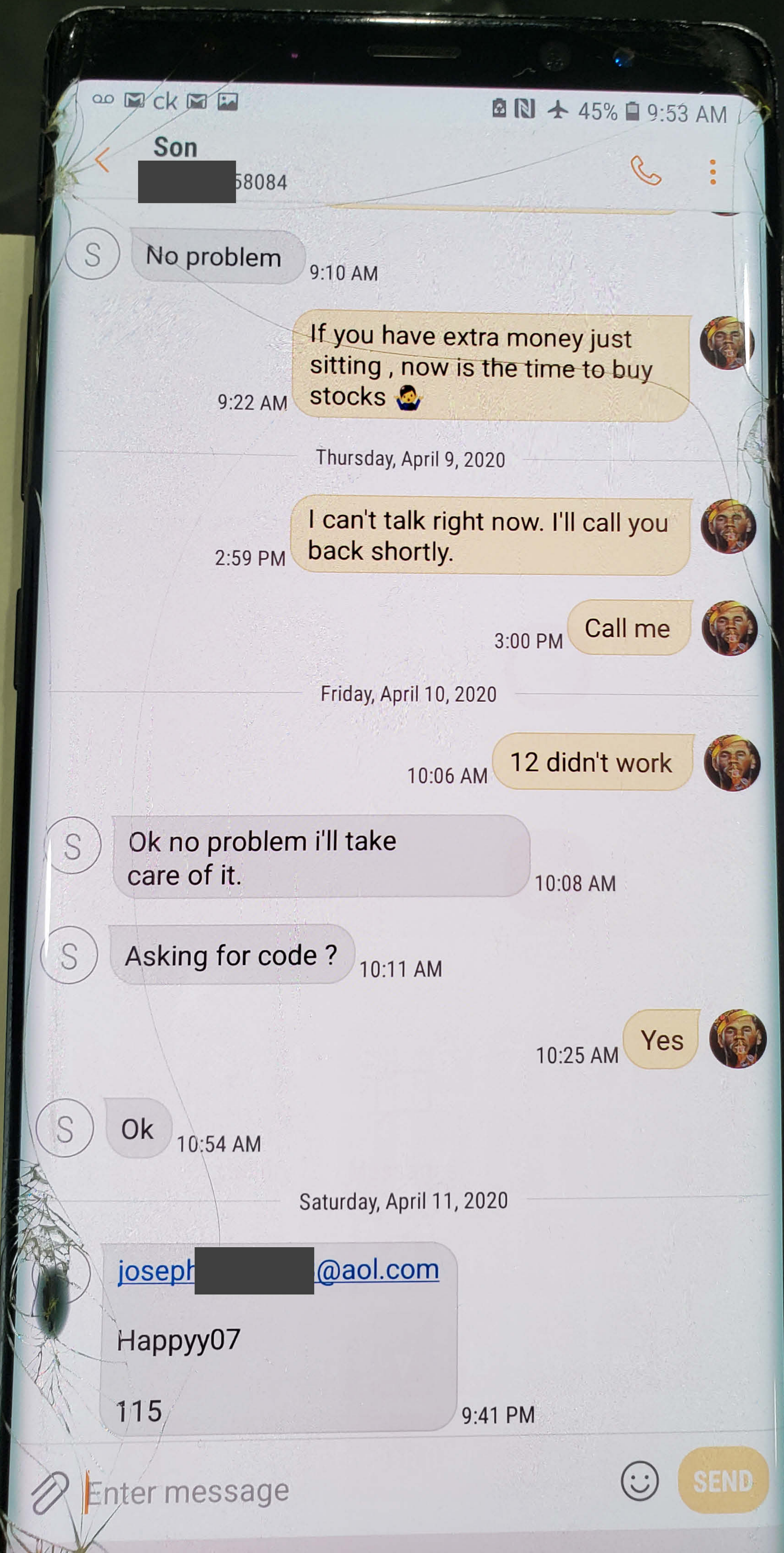
9:00 AM



Enter message



SEND



ck

45% 9:53 AM

Son

58084

S

No problem

9:10 AM

If you have extra money just sitting , now is the time to buy stocks 🙏

9:22 AM

Thursday, April 9, 2020

I can't talk right now. I'll call you back shortly.

2:59 PM

3:00 PM Call me

Friday, April 10, 2020

12 didn't work

10:06 AM

S

Ok no problem i'll take care of it.

10:08 AM

S

Asking for code ?

10:11 AM

Yes

10:25 AM

S

Ok

10:54 AM

Saturday, April 11, 2020

[joseph\[REDACTED\]@aol.com](#)

Happy07

115

9:41 PM



Enter message



SEND

0000

10:11 PM

3

Thank you bro

10:11 PM

10:12 PM

Anytime see if you can come
back in 3 weeks

Monday, June 8, 2020

3

About if I'm coming July 2 and
come back July 8

8:35 AM

Tuesday, June 9, 2020

3

No change fee

8:58 PM - 8:58 PM

\$379

JetBlue Airways

1h 1m nonstop

✈️ 📅 📅

8:58

FLY

Economy: Restrictions apply

No change fee

8:00 PM - 8:12 PM

\$379

JetBlue Airways

1h 12m nonstop

✈️ 📅 📅

8:00

FLY

Economy: Restrictions apply

No change fee

8:01 AM - 12:05 PM

\$487

American Airlines

4h 4m (1 stop)

✈️ 📅 📅

MMS

4:40 PM

Ticket is expensive bro

4:41 PM

why so high?

4th of July that's why

Son

8084



8:36 PM

Ok



Tuesday, June 23, 2020

8:56 PM

Video call me



Saturday, June 27, 2020

10:32 AM

15 min



S

Can I call you later?

11:34 AM

Thursday, July 2, 2020

3:21 PM

You good ?



Friday, July 3, 2020

S

Summerlake dr Davie
FL 33314

12:23 AM

5:59 AM

2 min away



Saturday, July 4, 2020

NW 99th Terrace, Sunrise,
FL 33322



4:09 AM

Thank you

4:09 AM

Sorry for late call

4:10 AM

No problem, it's late



Son

8084

MMS



MMS
7:29 PM



MMS
7:30 PM

41 mm diamond dial rolex

7:31 PM



Enter message



SEND

Son

8084

7:31 PM

41 mm diamond dail rolex

Rolex Day-Date II 41mm
Yellow Gold President Factory
Diamond Dial 218238 | eBay
<https://www.ebay.com/itm/Rolux-Day-Date-II-41mm-Yellow-Gold-President-Factory-Diamond-Dial-218238-/174088466278>



Rolex Day-Date II 41mm Yel-
Reference No. 218238. Rolex warranty no...
<https://www.ebay.com/itm/Rolux-Day-Date-II-41mm-Yellow-Gold-President-Factory-Diamond-Dial-218238-/174088466278>

7:33 PM



MMS
7:37 PM

Enter message



SEND

Son

8084

[prmd=sinv&sxsrf=ALeKk02X70W082uMw6PySTSX09Djr8srbg:1597103300779&source=Inms&tbm=isch&sa=X&ved=2ahUKEwiq6KW36ZHrAhXykOA KHWyGCioQ AUoAnoECBcQAg&biw=412&bih=718&dpr=2.63](https://www.google.com/search?q=f+n+...)

f n firearm - Google Search

7:48 PM

<https://www.google.com/search?q=f+n+...>

Thursday, August 20, 2020

4:01 PM

FLY PROPERTIES BOYZ LLC



4:05 PM

[134th St, North Miami, FL 33161](#)



4:14 PM

FLY BOYZ PROPERTIES LLC



Sunday, September 6, 2020

9:41 PM

Call in a few



S

No problem

9:42 PM

Thursday, September 24, 2020

3:45 PM

Hold on son sorry



Thursday, October 8, 2020

S

Can I call you later?

5:10 PM



Enter message



SEND

EXHIBIT 2

AFFIDAVIT

I, Matthew J. Riportella, do under oath depose a state:

I. INTRODUCTION

Agent Background

1. I am a Special Agent of the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since June 2012. I am currently assigned to the FBI Boston Division's Providence Rhode Island Complex Financial Crimes Task Force ("PRICFCTF"), which is comprised of law enforcement officers from the FBI, Rhode Island State Police ("RISP"), United States Secret Service ("USSS") and other federal law enforcement agencies. As a member of the PRICFCTF, I am responsible for investigating white collar crimes in Rhode Island. Previously, I was assigned to the FBI Boston Divisions' Organized Crime Task Force. I have experience investigating illegal gambling, narcotics, extortion, money laundering, kidnapping, wire fraud, mail fraud and other federal crimes. My investigations have included the use of surveillance techniques, and the execution of search, seizure, and arrest warrants.

Purpose

2. I make this affidavit in support of an application for an arrest warrant and criminal complaint charging Luckson LOUISSAINT (LOUISSAINT), DOB February 3, 1990, Social Security Number: 347-95-8779, with Conspiracy to Commit Mail, Wire, and Bank Fraud (18 U.S.C. § 1349), Access Device Fraud (18 U.S.C. § 1029(a)(5)), and Aggravated Identity Theft (18 U.S.C. § 1028A) ("Specified Federal Offenses"). LOUISSAINT resides at 49 Coyle Ave. #5 Pawtucket, RI and is described as a Black male, 31 years old, 5'7, weighing approximately 160 pounds with dark hair (hereinafter referred to as the "SUBJECT PERSON").

3. I also make this affidavit in support of Applications for a Search Warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a search of:

- a. the SUBJECT PERSON, Luckson LOUISSAINT, as more particularly described in Attachment A-1 (attached hereto and incorporated herein by reference) at whatever location

he may be found, for the items described in Attachment B-1;
and

- b. 49 Coyle Ave. #5 Pawtucket, RI (the SUBJECT PREMISES),
as more particularly described in Attachment A-2 (attached
and incorporated herein by reference) for the items
described in Attachment B-2,

4. As set forth below, there is probable cause to believe that located on the SUBJECT PERSON and in the SUBJECT PREMISES is evidence, fruits, and instrumentalities of violations the Specified Federal Offenses.

5. The facts set forth in the Affidavit are based on my personal observations, my training and experience, information obtained from other agents, witnesses, and records obtained during the course of the investigation. Because I submit this Affidavit for the limited purpose of showing probable cause, I have not included in this Affidavit each and every fact that I have learned in this investigation. Rather, I have set forth only facts sufficient to establish probable cause to issue an arrest warrant for the individuals identified herein and to search the email accounts set forth herein. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. PROBABLE CAUSE

6. As described herein, from at least March 2020 through October 2020, LUCKSON LOUISSAINT has conspired with James Legerme, Tony Mertile, and others, to provide information and receive fraudulently issued debit cards, all in furtherance of the receipt of fraudulent UI benefits.

A. Post- CARES Act Unemployment Fraud Schemes in Rhode Island and Nationwide.

7. Since early April 2020, the FBI, RISP, Internal Revenue Service-Criminal Investigations ("IRS-CI"), Department of Labor- Office of Inspector General ("Labor-OIG"), United States Postal Inspection Service ("USPIS") and the United States Secret

Service ("USSS"), with the assistance of other federal agencies, have been investigating a large volume of fraudulent UI claims submitted to the Rhode Island Department of Labor & Training ("RIDLT") and other state UI benefit agencies. These claims were submitted online using an individual's personally identifiable information ("PII") to include their name, DOB and SSN. These claims were paid out by the State of Rhode Island and other state UI agencies via electronic bank or wire transfers to bank accounts and/or to debit cards, identified by the applicant when the application for UI benefits was submitted.

UNEMPLOYMENT INSURANCE

8. Benefits that were available in 2020 and 2021 through state unemployment insurance agencies, such as RIDLT, included the traditional unemployment insurance benefits, as well as benefits that became available as federal legislation was passed at the outset and during the pendency of the COVID-19 pandemic. Because the conduct described herein involves various types of UI benefits sought from and paid by multiple state UI agencies, I have summarized some of these benefit programs.

9. The Unemployment Insurance Program ("UI Program") is a joint federal-state partnership administered on behalf of the U.S. Department of Labor by state workforce agencies ("SWA"), also commonly referred to as UI agencies, in each state. In Rhode Island, the UI Program is operated by the RIDLT, the RI UI agency / SWA. The UI Program is designed to provide benefits to persons who are out of work through no fault of their own. UI benefits are generally funded through state employment taxes paid by employers. In order to qualify for traditional UI benefits, the applicant must have earned wages which were taxed, for a qualifying period of time. Self-employed individuals, independent contractors and non-traditional workers whose income is outside of a traditional employment relationship (sometimes referred to as gig employees) not paying employment taxes, are generally not covered by UI programs.

10. On March 27, 2020, the CARES Act provided additional assistance to workers who would otherwise not qualify for traditional UI benefits. The CARES Act provided assistance in the form of Pandemic Unemployment Assistance ("PUA"),

Pandemic Emergency Unemployment Compensation ("PEUC") and Federal Pandemic Unemployment Compensation ("FPUC").

11. PUA generally provides benefits to certain individuals who would not qualify for traditional UI programs, and are unemployed, partially unemployed, or unable to work due to COVID-19 related reasons. Individuals who are able to telework with pay are not eligible for PUA assistance. PUA initially provided up to 39 weeks of benefits to qualifying individuals which were set to expire on December 31, 2020. On or about December 27, 2020, the Continued Assistance for Unemployed Workers of 2020 Act was signed into law. This Act extended the payment of PUA benefits for up to 50 weeks through March 14, 2021. Then on March 11, 2021, the American Rescue Plan Act of 2021 ("ARPA") was signed into law. Under ARPA, PUA benefits for up to 79 weeks have been extended through September 6, 2021. The PUA program is administered by the SWA / UI agency in each state, but the benefits are 100% funded by the federal government. A PUA claim is a claim for benefits against income earned or expected to be earned by the claimant in a particular state. The claimant must certify to the particular SWA / UI agency administering the benefits that the claimant is able to go to work each day, and, if offered a job, the claimant must be able to accept it. The claimant must certify this information on a weekly basis during the benefits period. The claimant is also responsible for reporting any income earned on a weekly basis to the SWA / UI agency to which they submitted a claim.

12. PEUC was established to extend the term for UI benefits and provided up to an additional 13 weeks of UI benefits to individuals who have exhausted their regular UI benefits under state or federal law and have no rights to UI under any other federal state or law. Under the Continued Assistance for Unemployed Workers of 2020 Act, PEUC benefits were extended to provide an additional 11 weeks of benefits for a maximum of 24 weeks through March 14, 2021. Under ARPA, PEUC benefits have been extended for up to 53 weeks through September 6, 2021.

13. Separately, FPUC provided an additional \$600 per week in benefits through July 2020, to individuals who were collecting UI, PUA and PEUC benefits.

FPUC benefits are 100% funded by the federal government. From August 1, 2020 through September 5, 2020, PUA and UI claimants were eligible to receive Federal Lost Wage Assistance ("FLWA") in the amount of \$300 per week funded by the Federal Emergency Management Agency ("FEMA"). Under the Continued Assistance for Unemployed Workers of 2020 Act, an additional \$300 in weekly FPUC benefits was extended from December 26, 2020 through March 14, 2021. Then under ARPA, FPUC benefits of \$300 have been extended through September 6, 2021.

LOUISSAINT is Identified as a Co-Conspirator

14. In our investigation, Tony Mertile, Junior Mertile, James Legerme, and Allen Bien-Aime, all residents of Florida, were identified as persons who were conspiring to use bank accounts to receive payments for fraudulent UI claims submitted to the RIDLT and to other state SWAs/UI systems and for fraudulent tax refunds; fraudulently access the bank accounts opened using PII of other persons and into which those fraudulently obtained funds were deposited; and withdraw fraudulently obtained UI benefits and tax refunds from the fraudulently opened bank accounts.

15. On October 6, 2020, Tony Mertile, Junior Mertile, James Legerme, and Allen Bien-Aime were all charged by Complaint in the District of Rhode Island in connection with a scheme to obtain fraudulent UI and tax refund proceeds.¹ On October 13, 2020, the residences of Tony Mertile, Junior Mertile, James Legerme, as well as their persons and vehicles, were searched pursuant to federal search warrants. In addition to multiple computers and cell phones, law enforcement agents located:

- a. At James Legerme residence, 2949 NW 99th Terrace, Sunrise, FL (Legerme's residence) -- approximately \$100,000 worth of jewelry and watches; \$73,758 cash and money orders, multiple cellular

¹ The Complaints for Tony Mertile, Junior Mertile, James Legerme, and Allen Bien-Aime are docketed at Dkt Nos. 20-MJ-95, 20-MJ-96, 20-MJ-97, and 20-MJ-98. The cases were later charged by Indictment and Superseding Indictment, in the District of Rhode Island. See Dkt. No. 20-CR-00100.

telephones, and over one hundred debit cards in the names of other persons, including Chime debit cards and mailers.

- b. At Tony Mertile's residence -- approximately \$940,000 in cash, firearms, a large collection of jewelry and watches; a large number of debit cards in the name of other persons, from multiple banks, including Chime Bank, Wells Fargo bank, and SunTrust bank; multiple flip style cell phones marked with telephone numbers, including with Rhode Island area code (401); a notebook that appears to identify Green Dot and Go Bank accounts, among others.
- c. At Junior Mertile's residence, -- \$125,000 in cash, debit cards in the names of other persons, and multiple cell phones.

16. During a preview search of a cellular telephone located at (Legerme's residence, agents viewed text messages between the user of the telephone, believed to be Legerme and a contact identified as "Son" with telephone number +4015458084. The telephone number 4015458084 has been identified as one used by LUCKSON LOUISSAINT. The telephone number 4015458084 is the phone number listed in the subscriber information with Apple for an account in the name of "Luckson Louissaint" at "49 coyle avenue, apt 5, pawtuket [sic], Rhode Island" with the Apple ID lucksonlouissaint@icloud.com. That phone number is also listed in the AirBNB user account for Luckson Louissaint. I also note that the contact information assigned to the number in cell phone located at Legerme's residence is "Son," which I believe to be an abbreviation for Luckson.

17. Based on the text messages exchanged between LOUISSAINT and Legerme, I believe that LOUISSAINT was provided Legerme, and his co-conspirators, with emails addresses and passwords to use in furtherance of the efforts to open fraudulent bank accounts and obtain fraudulent UI proceeds. Excerpts of some of the

messages are set forth below. In the messages, I have referred to the user of the cell phone as "Legerme" because the cell phone was found at his residence.

18. A text exchange dated March 28, 2020 reads:

-Legerme: 2:12 PM - You'll be done today?

-LOUISSAINT: 2:21 PM - Lebonjonas@aol.com

Happyy05

60

Based on my training and experience, in this text message, I believe that LOUISSAINT was providing Legerme with an email address and password to access that email account.

19. A text exchange dated April 2, 2020 reads:

-Legerme: 2:59 PM - Still have 20 left but I'm giving it to t but I need lol (Emoji)

-LOUISSAINT: 2:59 PM - ok 100 more

-LOUISSAINT: 3:00 PM - ?

-Legerme: Yes go ahead, I owe you 200, P owe 100, Fat 100, T 100 right now.

Based on my training and experience, in this text message, I believe that Legerme was telling LOUISSAINT that he still had email addresses and passwords to be used, but that he was giving those email addresses/passwords to "t," who I believe to be co-conspirator Tony Mertile. I also believe that LOUISSAINT was confirming additional activity between them with his statement "ok 100 more." I also believe that Legerme was confirming what he and his co-conspirators owed LOUISSAINT, specifically that he (Legerme) owed LOUISSAINT \$200 or owed for 200 email addresses and that his three co-conspirators, referenced by initials, owed him \$100 each or for 100 email addresses. At this point, whether the numbers refer to amounts owed or email addresses created, for which money is owed, is not yet known. I also note that in text messages between Legerme and LOUISSAINT on March 22 and 23, 2020, there were references to "P/200, G/100/Fat/100. Text exchanged I owe you 200, P owe 100, Fat 100, T 100". I believe the references to "P," "Fat," "G," and "T," refer to Legerme's co-conspirators, including Junior Mertile, who is known by the name "Peanut," and Tony Mertile, who is referred to as "T."

20. A text exchange from April 4, 2020 reads:

-Legerme: I never paid you for Tony first 20
-LOUISSAINT: Emelynwenderli76@aol.com
Happy06

Based on my training and experience, in this text message, I believe that Legerme was telling LOUISSAINT that he owes LOUISSAINT money on behalf of co-conspirator TONY MERTILE for LOUISSAINT for LOUISSAINT's part in providing information, including e-mail addresses, to Legerme and others.

21. A text exchange from April 10, 2020 reads:

-Legerme: 10:06 AM - 12 didn't work
-LOUISSAINT: 10:08 AM - ok no problem
10:11 AM - asking for code?
-Legerme: 10:12 – yes

Based on my training and experience, in this text message, I believe that Legerme was telling LOUISSAINT that 12 of the email accounts and passwords that he provided didn't work and that when JAMES Legerme tried to access the accounts, he was prompted to enter a code.

18. A text message from June 6, 2020 reads:

-Legerme: 9:24 PM – Getting the money now for you
-LOUISSAINT: 10:38 PM – ok

Based on my training and experience, I believe that Legerme was advising LOUISSAINT that he was obtaining payment for him.

22. I have also reviewed bank records from Wells Fargo, that show that an account was opened in the name of Ryan Fitzpatrick, DOB 2/4/1996, listing LOUISSAINT's residence in Pawtucket, Rhode Island as the customer address. I have confirmed that Ryan Fitzpatrick, with that DOB, is a real person and he does not reside in Pawtucket, Rhode Island. Based on my training and experience, I believe that a debit card for the Ryan Fitzpatrick account would have been sent to the address on file. From materials provided by Wells Fargo, this account and others, appear to be connected to

Tony Mertile, Legerme, and Junior Mertile. However, I note that the he investigation into the Wells Fargo activity is ongoing.

23. US Postal Service Records show that a priority mail parcel was sent, listing LOUISSAINT's home address and telephone number, 401-545-8084, to Legerme on August 25, 2020. A second parcel, a priority mail flat rate envelope, was sent from LOUISSAINT's address, the label image is partially cut off and no sender name can be seen, to Legerme on August 22, 2020. Based on my training and experience, and work on this investigation, I believe that LOUISSAINT was sending Legerme debit cards and/or PII for use in furtherance of the Specified Federal Offenses.

The October 13, 2020 Coyle Ave Search of LOUISSAINT's residence

24. On October 13, 2020, the Honorable Patricia A. Sullivan, US Magistrate Judge for the District of Rhode Island authorized search warrants for LOUISSAINT's residence, 49 Coyle Ave #5 Pawtucket, RI, and his person of LOUISSAINT.² On October 13, 2020, the FBI executed the search of LOUISSAINT's residence. Agents were unable to execute the search of his person because LOUISSAINT was not home at the time of the search of his residence. A woman who identified herself as LOUISSAINT's girlfriend told agents that LOUISSAINT was working.

25. During the search of LOUISSAINT's residence, agents found 3 Chime debit cards with the debit card mailers, in the names of Stevan Harris, Shane Harris and Shawn Harris addressed to 49 Coyle Ave #5 Pawtucket, RI.

26. I know from my training and experience that Chime is a financial technology company that offers overs on-line and app-based banking services. Banking services for Chime accounts and debit cards are provided by Stride Bank and Bancorp Bank. Records produced by Stride Bank and Bancorp showed that each of these cards were issued in three different names, using SSNs and DOBs of three real persons, and

² Case Numbers: 20-SW-375-PAS and 20-SW-376-PAS

all were sent to LOUISSAINT's residence. We have not yet determined if these numbers and emails are legitimate with whom that are associated.

27. Stride Bank records showed that:

- a. A person applied for the debit card in the name of Stevan Harris on June 17, 2020 at 1:55 pm, using SSN 533-17-3409 and DOB 7/28/1984. The listed account address was 49 Coyle Avenue, Pawtucket, RI 02860.³ An \$8,121.00 payment from Arizona Benefitpay, which services the Arizona UI agency, was made to this debit card on June 18, 2020. The AZ UI payment was for a claim filed on June 17, 2020 in the name of Shannon Harris, SSN 600-48-6910, with a listed Arizona address. I have confirmed that a Shannon Harris, with this SSN, lives in Washington. The application information for each of the debit cards listed a phone number and email.
- b. A person applied for the debit card in the name of Shane Harris on June 17, 2020, at 1:47 pm (8 minutes before the Stevan Harris application), using SSN 538-96-9491 and DOB 04/01/1985. The records from Stride Bank show no deposits on the debit card in the name of Shane Harris.⁴

28. Bancorp records showed that a Chime debit card in the name of Shawn Harris issued on June 17, 2020. The applicant listed the name Shawn Harris, and the SSN ending 1058 and DOB of 04/04/1985.⁵ The records from Bancorp show no deposits on the debit card in the name of Shane Harris. According to Bancorp records,

³ The listed phone number on the Stevan Harris Stride (Chime) account was 2532710737 and the email was miguelpolo@aol.com.

⁴ The listed phone number on the Stevan Harris Stride (Chime) account was 2533075942 and the email was juanaviel@aol.com.

⁵ The listed phone number on the Shawn Harris Bancorp (Chime) account was 2062518157 and the email was raulosua@aol.com.

the debit card in the name of Shane Harris was directed to be sent to "SHAWN HARRIS, 49 COYLE AVE APT 5, PAWTUCKET, RI 02860."

29. From my training and experience, and work on this investigation, I believe that the debit cards on which no deposits were made were opened to receive fraudulent UI benefits but we obtained the cards before they were used for that purpose.

Use of Real Identities

30. In addition to the use of the name Shannon Harris, as described above, in connection with the AZ UI claim, I have confirmed that the identifiers used to open the 3 Chime debit cards that were sent to LOUISSAINT's house all belong to real persons, whose DOBs and SSNs match the information use to open the accounts. None of the persons reside in LOUISSAINT's residence, the location listed as the address upon opening of the debit card accounts.

- a. The true name, DOB, and SSN 533-17-3409 of Stevan Harris were used to open and the Stride Bank issued Chime card found at LOUISSAINT's residence and on which \$8,121.00 in Arizona UI benefits were paid. Stevan Harris resides in Washington State.
- b. The true name, DOB, and SSN of Shane Harris were used to open and the Stride Bank issued Chime card found at LOUISSAINT's residence and on which \$8,121.00 in Arizona UI benefits were paid. Shane Harris resides in Oregon.
- c. The true name and DOB of Shawn Harris were used to open the Bancorp issued Chime card found at LOUISSAINT's residence. Shawn Harris is a resident of Washington state, not of LOUISSAINT's residence in Pawtucket, Rhode Island.

Statement by LOUISSAINT

31. On October 21, 2020, LOUISSAINT called your affiant at the FBI Providence Office and asked to discuss the search warrant that had been executed at his

home on October 13, 2021. LOUISSAINT claimed that James Legerme was his cousin and that the package that LOUISSAINT sent to Legerme in Florida was a gift card. I note that the mail records obtained to date show that LOUISSAINT sent two, not one mailings, to Legerme, in August. LOUISSAINT spent \$26.35 to send one parcel, and \$7.75 to send the second parcel.

32. LOUISSAINT also claimed that he did make email addresses for Legerme, but it was for Legerme to use to give his business and AirBNBs good reviews. LOUISSAINT claimed he made 20 emails at one time and 20 or 30 email addresses another time. According to records from AirBNB, Legerme is not an AirBNB host. Legerme's wife, Shemka Williams is a host of one AirBNB property in Fort Lauderdale, FL. However, AirBNB records show that there are only 13 reviews for that property, and the last five reviews were March 1, March 11, March 15, March 21, and April 3, 2020. I note that LOUISSAINT's and Legerme's messages described above occurred between March 22, 2020 and June 6, 2020.

33. LOUISSAINT also acknowledge that he knew Tony Mertile. He claimed that both Legerme and Tony Mertile helped him when he first came to the country and was down on his luck. LOUISSAINT said that the last time he spoke to Tony Mertile was in 2017 when he called him to wish him a happy birthday.

34. Based on my training and experience in investigating this and similar violations of federal law, I believe that LOUISSAINT is a willing participant involved the UI fraud. I believe that LOUISSAINT assisted Legerme, Tony Mertile, Junior Mertile and others commit UI fraud by making email addresses for them. I believe that LOUISSAINT was paid for his services for making these emails and that is what is referenced in the text messages between Legerme and LOUISSAINT referenced in the October 2020 Riportella Affidavit. I believe that the Chime card located inside LOUISSAINT's apartment with the \$8,121 of Arizona BenefitPay was payment for his services.

Additional UI Claims Associated with LOUISSAINT's Address

35. I am also aware that additional UI claims, in Rhode Island and in other states, list other persons and apartments in 49 Coyle Avenue, Pawtucket in UI applications. The IP addresses used to file those UI claims may be linked to additional UI claims for other addresses in multiple states. Our investigation is ongoing and we have not yet determined if those claims are valid and/or connected to LOUISSAINT.

Summary

36. Based on my training and experience, I believe that LUCKSON LOUISSAINT is conspiring with others, including James Legerme, Tony Mertile, Junior Mertile, and others, in the commission of the Specified Federal Offenses by providing information, including e-mail addresses and passwords, to his co-conspirators to open bank accounts and file fraudulent UI claims, and that he is knowingly receiving debit cards that were fraudulently issued in the names of others, to receive fraud proceeds.

37. The investigation into LOUISSAINT's conduct is ongoing. From a preliminary review of data from the Department of Labor, Office of the Inspector General, LOUISSAINT appears to be connected, through co-conspirators, to fraudulent UI claims in multiple states. However, the respective roles of LOUISSAINT and his co-conspirators, and the full scope of the conduct has not yet been determined.

38. Although an earlier search was conducted at LOUISSAINT's residence, I believe that additional evidence may be located at his residence. The nature of this fraud involved a complex scheme in which debit cards were issued in the names of others, and cards were mailed to persons, including LOUISSAINT, to facilitate the fraud. I believe that one or more banks, or UI agencies, may have sent materials to LOUISSAINT since the October 13, 2021 search. Further, as discussed above, we did not obtain LOUISSAINT's cell phone when the warrant was executed on October 13, 2021. As discussed above, the cell phone was used in the commission of the offense, and I believe that information relating to the Specified Federal Offenses will be located on LOUISSAINT's cell phone.

Evidence Obtained During Residential Searches

39. Based on my training and experience, I know that during the course of residential searches, I and other agents have also found items of personal property that tend to identify the person(s) in residence, occupancy, control, or ownership of the SUBJECT PREMISES and computer devices located therein. Such identification evidence is typical of the articles people commonly maintain in their residences, such as canceled mail, deeds, leases, rental agreements, photographs, personal telephone books, diaries, utility and telephone bills, statements, identification documents, and keys.

40. Given the nature of this crime, I also believe it is reasonable to believe that the access devices, such as debit cards, and information relating thereto (names, social security numbers, passwords, online user log ins, etc.) would be maintained a place that allowed for safe storage, but ready access, such as a residence, for ATM or other debit transactions to be conducted shortly after the posting of fraudulent UI and/or tax refund payments to an account.

Evidence Relating to Fraud Offenses

41. Based on my training and experience and familiarity with investigations into fraud conducted by other law enforcement agents, I know the following:

- a. Individuals maintain in their homes, both in paper and electronic format, among other items, records regarding the receipt and expenditure of money, documents relating to the purchase of assets, and records pertaining to their employment or business, even if that business is an illicit business.
- b. Given the nature of fraud, I believe that participants in a long running fraud that involves several participants, more often than not, will keep records containing names, addresses, email addresses, and telephone numbers of co-conspirators, as well as targets and victims, amounts received from them, and amounts sent to co-conspirators. These records are necessary to further the

illicit fraud business and can be found in paper form or stored electronically in cell phones and other electronic devices. Owing to the long-term usefulness of such items, and tracking relative proceeds among co-conspirators, this type of evidence would likely be generated, maintained, and then possibly forgotten about and not disposed of.

- c. I also know that those who make use of stolen personal identification as part of their fraud schemes, will often keep lists of the stolen PII, and notations on how and when that identify may be used, and any passwords for that "identity." I am also aware that fraudsters often maintain such documents related to their criminal activities at their residences or other locations over which they have control for an extended period of time, due to the high value associated with stolen PII that has been successfully used.
- d. From training and experience, I know that individuals who amass proceeds from illegal activities routinely attempt to further that conduct and/or conceal the existence and source of their funds by engaging in financial transactions with domestic and foreign institutions, and others, through all manner of financial instruments, including cash, cashier's checks, credit and debit cards, money drafts, traveler's checks, wire transfers, etc. Records of such instruments, including ATM receipts, are oftentimes maintained at the individual's residence.
- e. There are many reasons why criminal offenders maintain evidence for long periods of time. First, to the offender, the evidence may seem innocuous at first glance (e.g. financial, credit card and banking documents, travel documents, receipts, documents reflecting purchases of assets, personal calendars, telephone and address directories, checkbooks, videotapes and photographs,

utility records, ownership records, letters and notes, tax returns and financial records, escrow files, telephone bills, keys to safe deposit boxes, packaging materials, computer hardware and software). To law enforcement, however, such items may have significance and relevance when considered in light of other evidence. Second, the criminal offender may no longer realize he/she still possesses the evidence or may believe law enforcement could not obtain a search warrant to seize the evidence. The criminal offender may also be under the mistaken belief that he/she has deleted, hidden or further destroyed computer-related evidence, which in fact, may be retrievable by a trained forensic computer expert. Thus, records and ledger-type evidence that one would think a prudent person might destroy because of its incriminatory nature are sometimes still possessed months or even years after the records were created.

- f. Based on my knowledge with respect to facts and circumstances in this investigation, as well as my experience and training relating to cases involving individuals engaged in fraud schemes, as well as my discussions with other agents who investigated such cases, I know that it is a common practice for individuals engaged in these illegal activities to maintain the items and records or documents as set forth in Attachments B-1 through B-2, whether maintained on paper, in hand-written, typed, photocopied, or printed form, or electronically on a computer or cell phone, hard disks, external drives, RAM, flash memory, CD-ROMS, memory sticks, USB drives, and other magnetic or optical media, or any other storage medium.

Training and Experience on Digital Devices

42. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

- a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.
- b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents, programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

- c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.
- d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

43. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

- a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.
- b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to,

one gigabyte can store close to 19,000 average file size (300kb)

Word documents, or 614 photos with an average size of 1.5MB.

44. The search warrant also requests authorization to use the biometric unlock features of a device, based on the following, which I know from my training, experience, and review of publicly available materials:

- a. Users may enable a biometric unlock function on some digital devices. To use this function, a user generally displays a physical feature, such as a fingerprint, face, or eye, and the device will automatically unlock if that physical feature matches one the user has stored on the device. To unlock a device enabled with a fingerprint unlock function, a user places one or more of the user's fingers on a device's fingerprint scanner for approximately one second. To unlock a device enabled with a facial, retina, or iris recognition function, the user holds the device in front of the user's face with the user's eyes open for approximately one second.
- b. In some circumstances, a biometric unlock function will not unlock a device even if enabled, such as when a device has been restarted or inactive, has not been unlocked for a certain period of time (often 48 hours or less), or after a certain number of unsuccessful unlock attempts. Thus, the opportunity to use a biometric unlock function even on an enabled device may exist for only a short time. I do not know the passcodes of the devices likely to be found in the search.
- c. Thus, the warrant I am applying for would permit law enforcement personnel to, with respect to any device that appears to have a biometric sensor and falls within the scope of the warrant: (1) depress the user's thumb- and/or fingers on the device(s); and (2) hold the device(s) in front of the user's face with her eyes open to activate the facial-, iris-, and/or retina-recognition feature.

- d. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

REQUEST FOR SEALING

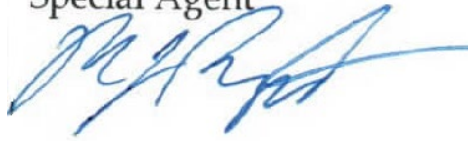
45. Because this investigation is continuing and disclosure of some of the details of this affidavit may cause the targets or other affiliated persons to flee or further mask their identity or activities, destroy physical and/or electronic evidence, or otherwise obstruct and seriously jeopardize this investigation, I respectfully request that this affidavit, and associated materials seeking this search warrant, be sealed until further order of this Court. Finally, I specifically request that the sealing order not prohibit information obtained from this warrant from being shared with other law enforcement and intelligence agencies.

CONCLUSION

46. For all of the reasons described above, there is probable cause to arrest Luckson LOUISSAINT for the Specified Federal Offenses and to believe that the items to be seized described in Attachment B-1 and B-2, will be found in a search of the SUBJECT PERSON and SUBJECT PREMISES described in Attachment A-1 and A-2.

I declare that the foregoing is true and correct.

Matthew J. Riportella
Special Agent



FEDERAL BUREAU OF INVESTIGATION

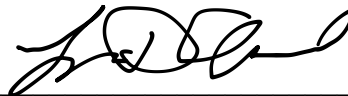
Attested to by the applicant in accordance with the requirements of Fed.
R. Crim. P. 4.1 by telephone.

May 24, 2021

Date

Providence, RI

City and State



Judge's signature

Lincoln D. Almond, US Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the

District of Rhode Island

United States of America

v.

LUCKSON LOUISSAINT, YOB: 1990

Case No. 1:21MJ59LDA

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of approx 3/2020 through 6/2020 in the county of _____ in the
_____ District of Rhode Island, the defendant(s) violated:

Code Section

18 U.S.C. § 1349; 18 U.S.C. §
1029(a)(5); and 18 U.S.C. § 1028A

Offense Description

Conspiracy to commit mail, wire, & bank fraud; Access device fraud; and
Aggravated Identity Theft

This criminal complaint is based on these facts:

See the attached Affidavit of Federal Bureau of Investigation ("FBI") Special Agent Matthew J. Riportella

☒ Continued on the attached sheet.Matthew J. Riportella
Special Agent

Complainant's signature

FBI Special Agent Matthew J. Riportella

Printed name and title

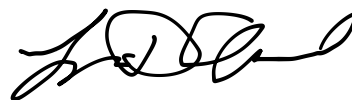
Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by

(specify reliable electronic

Telephone

May 24, 2021

Date: _____

City and state: Providence, Rhode Island

Judge's signature

Lincoln D. Almond, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT

for the
District of Rhode IslandUnited States of America
v.
LUCKSON LOUISSAINT, YOB: 1990

Case No. 1:21MJ59LDA

Defendant

ARREST WARRANT

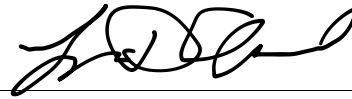
To: Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before a United States magistrate judge without unnecessary delay
(name of person to be arrested) LUCKSON LOUISSAINT, YOB: 1990,
who is accused of an offense or violation based on the following document filed with the court:

☐ Indictment ☐ Superseding Indictment ☐ Information ☐ Superseding Information ☐ Complaint
☐ Probation Violation Petition ☒ Supervised Release Violation Petition ☐ Violation Notice ☐ Order of the Court

This offense is briefly described as follows:

Conspiracy to commit mail, wire, & bank fraud; Access device fraud; and Aggravated Identity Theft - in violation of 18 U.S.C. § 1349; 18 U.S.C. § 1029(a)(5); and 18 U.S.C. § 1028A.

Date: May 24, 2021

Issuing officer's signature

City and state: Providence, Rhode IslandLincoln D. Almond, U.S. Magistrate Judge

Printed name and title

Return

This warrant was received on (date) _____, and the person was arrested on (date) _____
at (city and state) _____.

Date: _____

Arresting officer's signature

Printed name and title

**This second page contains personal identifiers provided for law-enforcement use only
and therefore should not be filed in court with the executed warrant unless under seal.**

(Not for Public Disclosure)

Name of defendant/offender: _____

Known aliases: _____

Last known residence: _____

Prior addresses to which defendant/offender may still have ties: _____

Last known employment: _____

Last known telephone numbers: _____

Place of birth: _____

Date of birth: _____

Social Security number: _____

Height: _____ Weight: _____

Sex: _____ Race: _____

Hair: _____ Eyes: _____

Scars, tattoos, other distinguishing marks: _____

History of violence, weapons, drug use: _____

Known family, friends, and other associates (*name, relation, address, phone number*): _____

FBI number: _____

Complete description of auto: _____

Investigative agency and address: _____

Name and telephone numbers (office and cell) of pretrial services or probation officer (*if applicable*): _____

Date of last contact with pretrial services or probation officer (*if applicable*): _____

UNITED STATES DISTRICT COURT
DISTRICT OF RHODE ISLAND

IN RE COMPLAINT

Misc. No. 1:21MJ59LDA

MOTION TO SEAL

The Government moves that this Motion to Seal and the attached documents (including the Complaint, Arrest Warrant, Cover Sheet, and Affidavit in Support) be sealed until further Order of this Court.

Respectfully submitted,

UNITED STATES OF AMERICA
By its attorneys,

RICHARD B. MYRUS
Acting United States Attorney



DENISE M. BARTON
Assistant U.S. Attorney
U.S. Attorney's Office
50 Kennedy Plaza, 8th FL
Providence, RI 02903
Tel (401) 709-5000
Fax (401) 709-5001
Email: Denise.Barton@usdoj.gov



STACEY P. VERONI
Assistant U.S. Attorney
U.S. Attorney's Office
50 Kennedy Plaza, 8th FL
Providence, RI 02903
Tel (401) 709-5000
Fax (401) 709-5001
Email: Stacey.Veroni@usdoj.gov

SO ORDERED:



LINCOLN D. ALMOND
UNITED STATES MAGISTRATE JUDGE
May 24, 2021

Dated: _____

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ INFORMATION ☐ INDICTMENT ☒ COMPLAINT

CASE NO. 1:21MJ59LDA

Matter Sealed: ☐ Juvenile ☐ Other than Juvenile☐ Pre-Indictment Plea ☐ Superseding ☐ Defendant Added
☐ Indictment ☐ Charges/Counts Added
☐ Information

Name of District Court, and/or Judge/Magistrate Location (City)

UNITED STATES DISTRICT COURT RHODE ISLAND
DISTRICT OF RHODE ISLAND Divisional OfficeName and Office of Person RICHARD B. MYRUS
Furnishing Information on ☒ U.S. Atty ☐ Other U.S. Agency
THIS FORM Phone No. (401) 709-5000Name of Asst. D. Barton/S. Veroni/G. Seaman
U.S. Attorney
(if assigned)

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)
Federal Bureau of Investigation☐ person is awaiting trial in another Federal or State Court
(give name of court)☐ this person/proceeding transferred from another district
per (circle one) FRCrP 20, 21 or 40. Show District☐ this is a reprosecution of charges
previously dismissed which were
dismissed on motion of:☐ U.S. Atty ☐ Defense☐ this prosecution relates to a
pending case involving this same
defendant. (Notice of Related
Case must still be filed with the
Clerk.)☐ prior proceedings or appearance(s)
before U.S. Magistrate Judge
regarding this defendant were
recorded underSHOW
DOCKET NO.MAG. JUDGE
CASE NO.Place of RHODE ISLAND
offense County

USA vs.

Defendant: LUCKSON LOUISSAINT

Address:

☐ Interpreter Required Dialect: _____Birth Date ☒ Male ☐ Alien
☐ Female (if applicable)

Social Security Number

DEFENDANT

Issue: ☒ Warrant ☐ Summons

Location Status:

Arrest Date _____ or Date Transferred to Federal Custody _____

☐ Currently in Federal Custody☐ Currently in State Custody☐ Writ Required☐ Currently on bond☐ Fugitive

Defense Counsel (if any): _____

☐ FPD ☐ CJA ☐ RET'D☐ Appointed on Target Letter☐ This report amends AO 257 previously submitted

OFFENSE CHARGED - U.S.C. CITATION - STATUTORY MAXIMUM PENALTIES - ADDITIONAL INFORMATION OR COMMENTS

Total # of Counts 3

Set	Title & Section/Offense Level (Petty = 1 / Misdemeanor = 3 / Felony = 4)	Description of Offense Charged	Felony/Misd.
	See Attached Sheet.	See Attached Sheet	<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor

UNITED STATES V. LUCKSON LOUISSAINT

**COMPLAINT COVER SHEET ATTACHMENT
MAXIMUM PENALTIES**

Count 1: (Conspiracy to Commit Mail, Wire, and Bank Fraud, 18 U.S.C. § 1349)

(Consp. to Commit Bank Fraud)

- a. 30 years imprisonment;
- b. \$1,000,000 fine;
- c. 5 years supervised release; and
- d. \$100 special assessment.

(Consp. to Commit Mail or Wire Fraud)

- a. 20 years imprisonment;
- b. \$250,000 fine, or twice the gross gain or loss;
- c. 3 years supervised release; and
- d. \$100 special assessment.

Count 2: (Access Device Fraud, 18 U.S.C. § 1029(a)(5))

- a. 15 years imprisonment;
- b. \$250,000 fine;
- c. 3 years supervised release; and
- d. \$100 special assessment.

Count 3: (Aggravated Identity Theft, 18 U.S.C. § 1028A)

- a. **Mandatory minimum** of 2 years imprisonment, consecutive to underlying felony; and
- b. \$100 special assessment.

DEFENDANT INFORMATION RELATIVE TO A CRIMINAL ACTION - IN U.S. DISTRICT COURT

BY: ☐ INFORMATION ☐ INDICTMENT ☒ COMPLAINTMatter Sealed: ☐ Juvenile ☐ Other than Juvenile☐ Pre-Indictment Plea ☐ Superseding ☐ Defendant Added
☐ Indictment ☐ Charges/Counts Added
☐ Information

Name of District Court, and/or Judge/Magistrate Location (City)

UNITED STATES DISTRICT COURT RHODE ISLAND
DISTRICT OF RHODE ISLAND Divisional OfficeName and Office of Person RICHARD B. MYRUS
Furnishing Information on ☒ U.S. Atty ☐ Other U.S. Agency
THIS FORM Phone No. (401) 709-5000Name of Asst. D. Barton/S. Veroni/G. Seaman
U.S. Attorney
(if assigned)

PROCEEDING

Name of Complainant Agency, or Person (& Title, if any)
Federal Bureau of Investigation☐ person is awaiting trial in another Federal or State Court
(give name of court)☐ this person/proceeding transferred from another district
per (circle one) FRCrP 20, 21 or 40. Show District☐ this is a reprosecution of charges
previously dismissed which were
dismissed on motion of:☐ U.S. Atty ☐ Defense☐ this prosecution relates to a
pending case involving this same
defendant. (Notice of Related
Case must still be filed with the
Clerk.)☐ prior proceedings or appearance(s)
before U.S. Magistrate Judge
regarding this defendant were
recorded underSHOW
DOCKET NO.MAG. JUDGE
CASE NO.Place of
offense RHODE ISLAND

County

CASE NO. 1:21MJ59LDA

USA vs.

Defendant: LUCKSON LOUISSAINT49 Coyle Ave. #5 Pawtucket, RI

Address:

☐ Interpreter Required Dialect: _____Birth Date 2/3/1990 ☒ Male ☐ Alien
☐ Female (if applicable)Social Security Number 347-95-8779

DEFENDANT

Issue: ☒ Warrant ☐ Summons

Location Status:

Arrest Date _____ or Date Transferred to Federal Custody _____

☐ Currently in Federal Custody☐ Currently in State Custody☐ Writ Required☐ Currently on bond☐ Fugitive

Defense Counsel (if any): _____

☐ FPD ☐ CJA ☐ RET'D☐ Appointed on Target Letter☐ This report amends AO 257 previously submitted

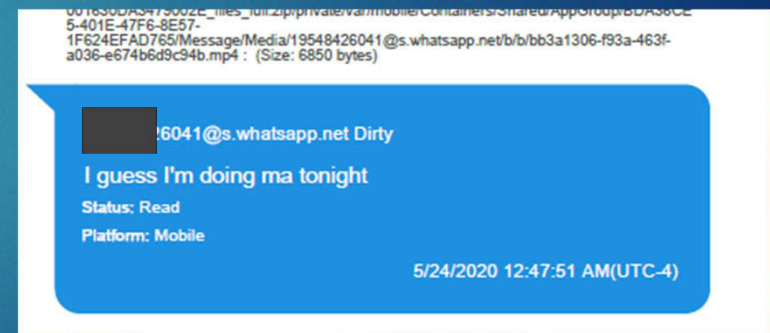
OFFENSE CHARGED - U.S.C. CITATION - STATUTORY MAXIMUM PENALTIES - ADDITIONAL INFORMATION OR COMMENTS

Total # of Counts 3

Set	Title & Section/Offense Level (Petty = 1 / Misdemeanor = 3 / Felony = 4)	Description of Offense Charged	Felony/Misd.
	See Attached Sheet.	See Attached Sheet	<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor
			<input checked="" type="checkbox"/> Felony <input type="checkbox"/> Misdemeanor

EXHIBIT 3

**Excerpts from Messages Between
Tony Mertile (██████████-3678)
and
James Legerme (“Dirty”) (██████████-6041)**



18

3678@s.whatsapp.net T

Allen
Miller
Freeman
Gibson
Haddad

Participant	Delivered	Read	Played
19548426041 @s.whatsapp.net Dirty	5/8/2020 6:32:21 PM(UTC-4)	5/8/2020 6:32:58 PM(UTC-4)	

Status: Sent
Platform: Mobile

5/8/2020 6:32:20 PM(UTC-4)

Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE
5-401E-47F6-8E57-1F624EFAD765/ChatStorage.sqlite : 0x0E98 (Table: ZWAMESSAGE,
ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE
5-401E-47F6-8E57-
1F624EFAD765/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist : 0x4E8
(Size: 13152 bytes)

3678@s.whatsapp.net T

Stewart
Fields
Park
Ryan

Participant	Delivered	Read	Played
19548426041 @s.whatsapp.net Dirty	5/8/2020 6:35:41 PM(UTC-4)	5/8/2020 6:35:41 PM(UTC-4)	

Status: Sent
Platform: Mobile

5/8/2020 6:35:40 PM(UTC-4)

Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE

Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE
5-401E-47F6-8E57-1F624EFAD765/ChatStorage.sqlite : 0x7F4C4 (Table: ZWAMESSAGE,
Size: 1327104 bytes)

3678@s.whatsapp.net T

Hit me

Participant	Delivered	Read	Played
19548426041 @s.whatsapp.net Dirty	5/18/2020 7:11:40 PM(UTC-4)	5/18/2020 8:00:10 PM(UTC-4)	

Status: Sent
Platform: Mobile

5/18/2020 7:11:40 PM(UTC-4)

Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE
5-401E-47F6-8E57-1F624EFAD765/ChatStorage.sqlite : 0x7F44E (Table: ZWAMESSAGE,
ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE
5-401E-47F6-8E57-
1F624EFAD765/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist : 0x4E8
(Size: 13152 bytes)

26041@s.whatsapp.net Dirty

Ohio
Kansas
P.a

Silva
Walker
Wilson
Green

Status: Read
Platform: Mobile

5/18/2020 8:00:53 PM(UTC-4)

Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-
401E-47F6-8E57-1F624EFAD765/ChatStorage.sqlite : 0x7FF09 (Table: ZWAMESSAGE,
ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

31

DRAFT

8041@s.whatsapp.net Dirty
What you taking about?? The waiter ? Or energy?
Status: Read
Platform: Mobile
7/8/2020 3:47:11 PM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E5FA (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

17864733678@s.whatsapp.net T
Did u check your yop
Participant Delivered Read Played
19548426041@s.whatsapp.net Dirty 7/8/2020 3:47:25 PM(UTC-4) 7/8/2020 3:47:55 PM(UTC-4)
Status: Sent
Platform: Mobile
7/8/2020 3:47:34 PM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E5FA (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

17864733678@s.whatsapp.net T
I sent u a Plastic list
Participant Delivered Read Played
19548426041@s.whatsapp.net Dirty 7/8/2020 3:47:51 PM(UTC-4) 7/8/2020 3:47:55 PM(UTC-4)
Status: Sent
Platform: Mobile
7/8/2020 3:47:51 PM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E5FA (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

8041@s.whatsapp.net Dirty
Ok you I see it
Status: Read
Platform: Mobile
7/8/2020 3:48:20 PM(UTC-4)

System Message System Message
Missed Voice Call
Platform: Mobile
7/11/2020 6:38:00 PM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E5FA (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

8041@s.whatsapp.net Dirty
Double check to see Anastasia on ... paid that one too
Status: Read
Platform: Mobile
7/11/2020 6:38:40 PM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E5FA (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

8041@s.whatsapp.net Dirty
Anastasia Freeman ?
Status: Read
Platform: Mobile
7/12/2020 12:40:51 AM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E5FA (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist : 0x4E8 (Size: 13152 bytes)

17864733678@s.whatsapp.net T
Front thing in the morning kills ima check that
Participant Delivered Read Played
19548426041@s.whatsapp.net Dirty 7/12/2020 1:11:51 AM(UTC-4) 7/12/2020 8:20:37 AM(UTC-4)
Status: Sent
Platform: Mobile
7/12/2020 1:11:45 AM(UTC-4)

Source Info:
00000020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0x4E43D (Table: ZWAMESSAGE, ZWAORUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

DRAFT

001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0xEFFB0 (Table: ZWAMESSAGE, Size: 1327104 bytes)

6041@s.whatsapp.net Dirty

Only 1 was good ... tried hitting you up for more ... I sent to the yop

Status: Read

Platform: Mobile

7/13/2020 7:39:06 AM(UTC-4)

Source Info:
00008020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0xEFE81 (Table: ZWAMESSAGE, ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

6041@s.whatsapp.net Dirty

Send more I guess and I'll update both today

Status: Read

Platform: Mobile

7/13/2020 7:46:41 AM(UTC-4)

Source Info:
00008020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0xEFD0B (Table: ZWAMESSAGE, ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0xED02D (Table: ZWAMESSAGE, ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

6041@s.whatsapp.net Dirty

Got 4 Freemans

Status: Read

Platform: Mobile

7/14/2020 12:34:39 AM(UTC-4)

Source Info:
00008020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0xED748 (Table: ZWAMESSAGE, ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)

3678@s.whatsapp.net T

Say less

Participant	Delivered	Read	Played
19548426041@s.whatsapp.net Dirty	7/14/2020 10:30:06 AM(UTC-4)	7/14/2020 10:32:33 AM(UTC-4)	

Status: Sent

Platform: Mobile

7/14/2020 10:26:10 AM(UTC-4)

Source Info:
00008020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/ChatStorage.sqlite : 0xED42E (Table: ZWAMESSAGE, ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)
00008020-001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BD436CE5-401E-47F8-8E57-1F824EFAD765/Library/Preferences/group.net.whatsapp.WhatsApp.shared.plist : 0x4E8 (Size: 13152 bytes)

DRAFT

0016300A3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA39CE
5-401E-47F8-8E57-1F624EFAD765/ChatStorage.sqlite : 0x5F36 (Table: ZWMESSAGE,
Size: 1327104 bytes)

6041@s.whatsapp.net Dirty

Attachments:



Size: 87969
File name: 3c35af18-3ae7-49b6-b1d6-73252c7cee5.jpg
Path: https://mmg.whatsapp.net/d/t/624EFAD765/ChatStorage.sqlite : 0x1033B6 (Table: ZWMESSAGE,
ZWAGROUPMEMBER, ZWCHATSESSION, Size: 1327104 bytes)
3c35af18-3ae7-49b6-b1d6-73252c7cee5.jpg

Status: Read
Platform: Mobile

7/22/2020 8:17:58 PM(UTC-4)

Source Info:

6041@s.whatsapp.net Dirty

Attachments:



Size: 106713
File name: 55b5a9a5-41ed-4900-8e97-e50c92e1e8e0.jpg
Path: https://mmg.whatsapp.net/d/t/624EFAD765/ChatStorage.sqlite : 0x1033B7 (Table: ZWMESSAGE,
ZWAGROUPMEMBER, ZWCHATSESSION, ZWAMEDIANTEM, Size: 1327104 bytes)
55b5a9a5-41ed-4900-8e97-e50c92e1e8e0.jpg

Status: Read
Platform: Mobile

7/22/2020 8:17:58 PM(UTC-4)

Source Info:

0016300A3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA39CE

6041@s.whatsapp.net Dirty

21k landed for us

Status: Read
Platform: Mobile

7/23/2020 7:43:02 PM(UTC-4)

6041@s.whatsapp.net Dirty

Status: Read
Platform: Mobile

7/26/2020 9:51:37 PM(UTC-4)

Source Info:
00008020-
0016300A3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA39CE
5-401E-47F8-8E57-1F624EFAD765/ChatStorage.sqlite : 0x1033B6 (Table: ZWMESSAGE,
ZWAGROUPMEMBER, ZWCHATSESSION, Size: 1327104 bytes)

6041@s.whatsapp.net Dirty

Attachments:



Size: 150036
File name: a0f18be7-72da-476f-9e4a-df3284dd07.jpg
Path: https://mmg.whatsapp.net/d/t/624EFAD765/ChatStorage.sqlite : 0x1033B7 (Table: ZWMESSAGE,
ZWAGROUPMEMBER, ZWCHATSESSION, ZWAMEDIANTEM, Size: 1327104 bytes)
a0f18be7-72da-476f-9e4a-df3284dd07.jpg

Status: Read
Platform: Mobile

7/27/2020 11:32:52 AM(UTC-4)

Source Info:
00008020-
0016300A3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA39CE
5-401E-47F8-8E57-1F624EFAD765/ChatStorage.sqlite : 0x1033B7 (Table: ZWMESSAGE,
ZWAGROUPMEMBER, ZWCHATSESSION, ZWAMEDIANTEM, Size: 1327104 bytes)
00008020-
0016300A3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA39CE
5-401E-47F8-8E57-1F624EFAD765/Message/Media/19548420041@s.whatsapp.net/a/01f0be7-72da-476f-

chime

Your Deposit Has Arrived!

Hi Alyssa,

A deposit of \$114,900.00 has posted
to your Spending Account. Your
updated balance is now \$114,900.00.

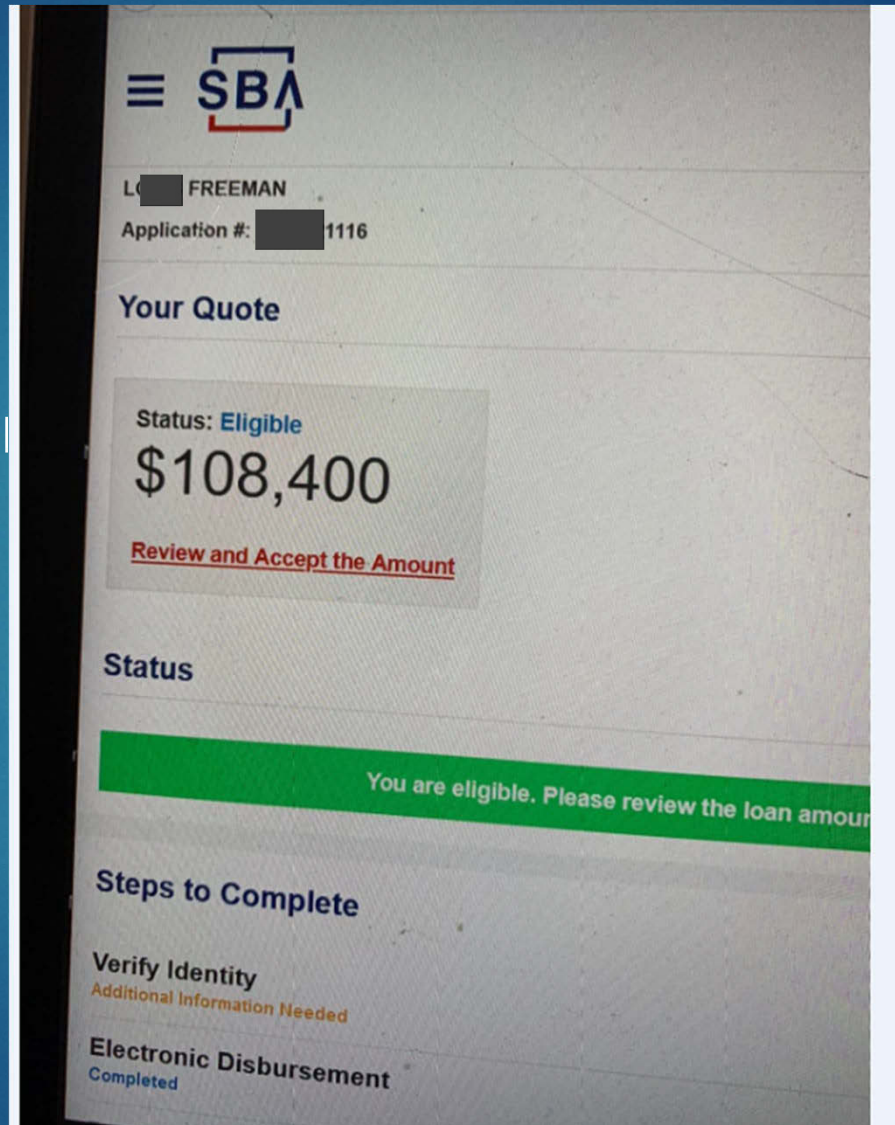
Congratulations on funding your
account! You can now use your
Chime Visa® Debit Card.

Cheers,
The Chime Team

DRAFT



Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/8DA36CE
5-401E-47F6-8E57-1F624EFAD765/ChatStorage.sqlite : 0x10792D (Table: ZWAMESSAGE,
ZWAMEDIATEM, ZWAGROUPMEMBER, ZWACHATSESSION, Show - 1377304 bytes)



DRAFT

678@s.whatsapp.net T

Attachments:



Size: 286413
File name: 391a6808-0a8a-46b9-8ded-7a2253757f0f.jpg
Path: https://mmg.whatsapp.net/d/f/AsDLdOSU7gg6rM6GES5iUJ3gR9p-vAwfS-Wikimyc.enc
391a6808-0a8a-46b9-8ded-7a2253757f0f.jpg

Participant	Delivered	Read	Played
19548426041 @s.whatsapp.net Dirty	8/3/2020 6:35:15 PM(UTC-4)	8/3/2020 6:50:28 PM(UTC-4)	


Status: Sent
Platform: Mobile

8/3/2020 6:35:12 PM(UTC-4)

Source Info:
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA36CE
5-401E-47F6-8E57-1F624EFAD765/ChatStorage.sqlite : 0x10C189 (Table: ZWAMESSAGE,
ZWAMEDIAITEM, ZWAGROUPMEMBER, ZWACHATSESSION, Size: 1327104 bytes)
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA36CE
5-401E-47F6-8E57-
1F624EFAD765/Library/Preferences/group.net.whatsapp.WhatsApp.plist : 0x4E8
(Size: 13152 bytes)
00008020-
001630DA3479002E_files_full.zip/private/var/mobile/Containers/Shared/AppGroup/BDA36CE
5-401E-47F6-8E57-
1F624EFAD765/Message/Media/19548426041@s.whatsapp.net/3/9/391a6808-0a8a-46b9-
8ded-7a2253757f0f.jpg : (Size: 286413 bytes)

17864733678@s.whatsapp.net T

Attachments:



Size: 321184
File name: 06f18b07-f265-4c4c-ac35-c08b7db5986b.jpg
Path: https://mmg.whatsapp.net/d/f/Aqr3Z7NeXh8N0FTBfo62D.KjwXsXOPT8Hr93SSuP89
e.enc
06f18b07-f265-4c4c-ac35-c08b7db5986b.jpg

Participant	Delivered	Read	Played
19548426041 @s.whatsapp.net Dirty	8/3/2020 6:47:36 PM(UTC-4)	8/3/2020 6:50:28 PM(UTC-4)	

In order to register you must have a valid Driver's License or a State ID Card. Please contact the IDES Claimant Services Center at (800) 244-5631 for further assistance.

Asterisk (*) indicates a required field

You have already registered with the Illinois Department of Employment Security. If you have forgotten your username and/or password, please [click here](#).

Identification Type	* Driver's License
Identification Number	* M [REDACTED] 0206
Issuing State	* Illinois
First Name (as listed on Identification)	* S [REDACTED]
Middle Initial (as listed on Identification)	[REDACTED]

Asterisk (*) indicates a required field

You have already registered with the Illinois Department of Employment Security. If you have forgotten your username and/or password, please [click here](#).

Identification Type	* Driver's License
Identification Number	* [REDACTED] 38
Issuing State	* Illinois
First Name (as listed on Identification)	* S [REDACTED]
Middle Initial (as listed on Identification)	[REDACTED]
Last Name (as listed on Identification)	* MIDDLETON
Birth Date (as listed on Identification)	* [REDACTED] 1943