IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Criminal Case No: 1:23-cr-00300-CNS

UNITED STATES OF AMERICA,

Plaintiff,

v.

1. IKPONMWOSA PERO ERHINMWINROSE,

Defendant.

GOVERNMENT'S TRIAL BRIEF

In advance of the pretrial conference, the government submits this trial brief to flag five potential legal issues that may arise during trial, while also noting how many of the issues could be resolved in advance of trial to make the trial more efficient and avoid wasting the Court's and jury's time on issues not relevant to the defendant's guilt.

1. **The Court can authenticate copies of data extracted from electronic devices without the need for live witnesses**

Three government witnesses will testify solely about copying data from devices:

- Senior Special Agent Umesh Patel performed two relevant downloads from devices belonging to Agbure.
- Digital Investigative Analyst Toshiro Muragaki performed two relevant downloads from devices belonging to Agbure.

Computer Scientist / Analyst Joshua Kulp performed seven relevant downloads from devices belonging to Tobore and two from items belonging to the defendant

The Court could streamline trial by ruling in advance of trial based on these agents' Rule 902(14) affidavits (Ex. 1) that this data is what it purports to be: a copy of data from an electronic device, storage medium, or file. As noted by the Advisory Committee on the Federal Rules of Evidence, Rule 902(14) reflects that "the expense and inconvenience of producing a witness to authenticate an item of electronic evidence is often unnecessary." Rule 902(14) includes a notice provision, and the government first provided notice to the defendant that it intended to authenticate these records by affidavit on October 28, 2025. Ex. 2. It did so a second time as part of its expert notice on November 8, 2025 and by a supplement on November 12, 2025 that informed the defendant that the government intended to offer all these copies of data through affidavit in accordance with Fed. R. Evid. 902(11), (13) and (14) and that, while it was noticing one of these affiants as an expert out of an abundance of caution, the witnesses would testify as fact witnesses because no expertise is required to testify about copying data from an electronic device. Ex. 3. The defendant did not dispute that the witnesses were lay witnesses within the Court's deadline but has insisted on live testimony for these foundational witnesses and opposes self-authentication of the data through the Rule 902(14) affidavits.

But requiring in-person testimony is unnecessary when the affidavits fully lay the foundation and make the copies self-authenticating. *See United States v. Judkins,* ECF No. 113, 21-cr-55 (Oct. 18, 2022) (concluding that data copied from an electronic devices is self-authenticating if accompanied by certification and citing cases from First, Second and Ninth Circuits); *United States v. Palmer*, 2025 WL 2978633, at *10

(S.D.N.Y. Oct. 21, 2025) (finding phone extracts self-authenticating without live testimony based on Rule 902(13) and (14) affidavit).

The defendant's objection to a valid Rule 902(14) affidavit is especially meritless where, as here, much of the content will be admitted before the foundational witnesses testify and other witnesses will testify as to the substance of the messages. Most device content at trial will come from devices belonging to Tobore, who is competent to testify about the authenticity of his own devices. *See United States v. Fluker*, 698 F.3d 988, 999 (7th Cir. 1999) (distinguishing between authentication by the author of content and through circumstantial evidence when the author does not testify). And because he can authenticate his own content, it's hard to see what value later putting on the foundation witnesses would have when the rules of evidence do not require it and the author of the content is available to testify. Second, the download and content of the devices was reviewed by Investigative Specialist Elizabeth Dale and Special Agent Matthew Zimmerman, both of whom the government will call as witnesses and who the defendant can cross examine about their testimony and conclusions.

The Court can streamline trial by ruling that data copied by these three agents—supported by affidavit—is self-authenticating. To the extent these affiants must provide live testimony—and based on the number of devices each will authenticate—the government anticipates it will amend its witness list to increase the time needed for direct testimony.

2. The Court can rule on the authenticity of content from electronic accounts and devices based on the record of the November 24, 2025 pretrial hearing

Apple, Google, and Microsoft ("providers") submitted declarations certifying that the records they produced meet the requirements of Rule 803(6). That is, the providers

created and maintained the texts and emails, they were kept by the providers as part of their regular business activities, and they were made as part of the providers' respective business. These declarations from the providers are thus sufficient to show that the texts and emails are authentic copies of records created and maintained by the providers. *See United States v. Ayelotan*, 917 F.3d 394, 402 (5th Cir. 2019) (finding that emails obtained from Google and Yahoo! accompanied by certification were admissible under Rule 803(6)).

But the providers do not create the *content* of the texts or emails they maintain in their businesses. The Court must also authenticate that content is what it purports to be: content from accounts of the defendant or coconspirators. *See, e.g., United States v. Gal*, 606 F. App'x 868, 874-75 (9th Cir. 2015) (affirming trial court ruling admitting emails where certification showed that Yahoo made record of email and other evidence established that defendant sent them).

Because a defendant usually does not authenticate his or her own electronic content, such content more typically is authenticated using Rule 901(b)(3) or 901(b)(4). *See, e.g., United States v. Barber*, 937 F.3d 965, 970 (7th Cir. 2019) (providing as examples for authenticating content on an online account under Rule 901 "the presence of a nickname, date of birth, address, email address, and photos" in the account); *Fluker*, 698 F.3d at 999 (7th Cir. 2012) (noting that electronic communications can be authenticated based on circumstantial evidence under Rule 901(b)(4)); *United States v. Tank*, 200 F.3d 627, 630-31 & n.5 (9th Cir. 2000) (concluding that there was sufficient evidence to authenticate emails under Rule 901, that any concerns about alteration or deletion were introduced by the defendant himself, and that such deletions would go to

weight of the evidence, not its admissibility); *United States v. Bertram*, 259 F. Supp. 3d 638, 642-644 (E.D. Ky. 2017) ("After considering the characteristics of the numerous emails at issue in this case as well as the context and background testimony provided by the authenticating witnesses, the Court has little doubt that the emails are exactly what they purport to be, and this remains true regardless of whether the authenticating witness was a sender or recipient.").

While the government's previous Notice of Federal Rule of Evidence 801(D)(2)(A) and (E) Statements (ECF No. 211) explained that the statements in each account are not hearsay, the same evidence also authenticates the content from the electronic accounts listed in ECF Nos. 211-1 and 211-2 under Rules 901(b)(3) and 901(b)(4). *Fluker* provides a good example: there, email addresses indicated that an email was sent by a member of "MTE," which was a business organization used by the conspirators. And the contents of those emails established that whoever sent the email had information that would only be known by an "insider." 698 F.3d at 999-1000. This was sufficient for the items to be authenticated and other rules of evidence—like the co-conspirator statement exception to the hearsay rule—provided a basis for admission. *Id.* at 1000. *See also United States v. Safavian*, 435 F. Supp. 2d 36, 40 (D.D.C. 2006) ("The Court notes that it is possible to authenticate these emails through examination of the contents, distinctive characteristics, and appearance, and others by comparison to authenticated e-mails, and the jury is free to make its own examinations and conclusions.").

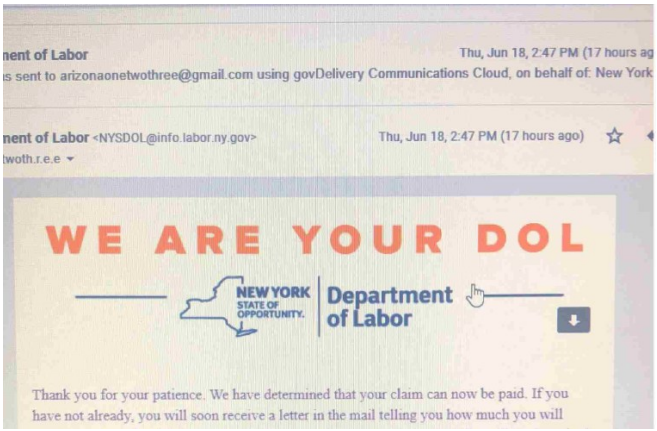
During the upcoming hearing on Rule 801(d)(2)(A) and (E) statements, the Court thus can consider the same evidence consisting of the government's proffer, agent

testimony, and all exhibits presented to both (i) authenticate the content under Rule 901(a), and (ii) make preliminary admissibility findings under the exceptions to the hearsay rule set forth in Rules 801(d)(2)(A), 801(d)(2)(E) and 803(6). Just as in *Barber, Fluker*, *Bertram,* and *Safavian* there is overwhelming circumstantial evidence under 901(b)(3) and (4) that the text and email content for the accounts in the government's proffer are authentic. The messages themselves include content that only "insiders" would know: they contain ties to the defendant and ledgers of identity-theft victim information used on applications for COVID-relief loans, tax refunds, and unemployment benefits. *See, e.g.,* ECF No. 211-3; ECF No. 211-6.

And unlike the usual case, the Court also can rely on Erhinwinrose's own words to authenticate the content in the accounts. He admitted in a proffer that he used the personal accounts in ECF No. 211-1, including icomo4real and ipemyp2. And those personal accounts uniquely connect him to the fraud accounts in the same exhibit, as laid out in other exhibits to ECF No. 211: (a) he previously used a version of his name, "Pero ik," as his display name for the ledger account (211-9, at 1-2), (b) he stored his birth certificate, school records, and photographs in the ledger account's Google Drive folders (211-9, at 3-8), (c) he searched emails in fraud accounts for his own name or emails he forwarded from his personal accounts (211-9, at 10-13), (d) he attached his credit report to a Google instant message to a coconspirator (211-9, at 9), (e) he accessed his ledger account from the same browser on the same computer he used to access his personal email and numerous other fraud email accounts (211-8), and (f) he used his own distinctive passwords and subject lines across personal and fraud accounts (211-4, 211-5, 211-10). In addition to saving screenshots of the ledger

account in his personal icomo4real gmail account (211-12), he also routinely saved to the icomo4real account's Google Photos folders screen captures (Ex. 4) documenting his crimes, including of a stack of $100 bills, emails from state unemployment agencies about fraudulent applications submitted using his facilitating accounts such as arizonaonetwothree, PII of identity theft victims used in the fraud and money laundering conspiracy, GoBank or GreenDot cards purchased by money runners, and advice he offered to subordinates about romance scams:





When Tobore's residence was searched in connection to his involvement in Erhinmwinrose's conspiracy, Erhinmwinrose replaced his old electronic devices in an attempt to destroy evidence, drove to Tennessee to help Tobore destroy evidence, and fled the country which is additional confirmation that he occupied the hub of the conspiracy wheel. *See* ECF No. 215. All of this evidence makes it more than apparent that the texts and messages are what they purport to be: communications between and among Erhinmwinrose, his co-defendants, and other coconspirators working together to rob the government of over $8 million.

Government exhibits also include files Google provided—such as the ledger accounts' log files containing Google chat or hangout messages and Google Drive file

paths—with the content rendered in a more readable and visually appealing way. Nothing about this rendering, whether done by manually by cutting and pasting relevant messages from the log file and putting them into a word file, rendering content more readable, or displaying the metadata such as date created or file path, changes this analysis related to authenticity. *See, e.g., United States v. Kilpatrick*, 2012 WL 3236727, at *6 (E.D. Mich. Aug. 7, 2012) (noting that government could take texts produced by cell phone company in excel file and extract them into WordPerfect to make them more readable). Using reliable software just saves time and makes the evidence accessible to the Court and the jury.

3. **The government will present two witnesses and has proposed a jury instruction because the defendant has not stipulated to venue for any counts**

Although the government proposed factual stipulations related to venue, the defendant has not agreed to any of them. *See* Ex. 5 (proposed factual stipulations). As a result, the government included two witnesses on its witness list who will testify about venue (and also will introduce testimony related to venue through other witnesses). The parties also have provided a stipulated jury instruction about venue, and the government anticipates that this is the instruction most likely to change based on the way evidence comes in based on the complicated legal questions and different standard of proof.

4. **The government will offer extensive summary exhibits based on admissible business records.**

A crime of this magnitude generates voluminous electronic content, financial records, and loan paperwork. The government intends to introduce summary exhibits prepared by agents based on their review of voluminous bank, cell-site, loan, tax, IP address, unemployment, and other records that are authentic business records

supported by business records certificates. *See* ECF No. 223, at 51-52 (1000 series exhibits); ECF No. 212 (Notice of Business Records Certificates).

Under Federal Rule of Evidence 1006, summary exhibits are routinely admitted through lay witnesses to summarize the contents of voluminous business and financial records. *See Harris Mkt. Rsch. v. Marshall Mktg. & Commc'ns, Inc.*, 948 F.2d 1518, 1525 (10th Cir. 1991) (recognizing that Rule 1006 "clearly permits the use of a summary of business records provided all of the records from which it is drawn are otherwise admissible"); *United States v. Caballero*, 277 F.3d 1235, 1247 (10th Cir. 2002) (lay financial analysis witness permitted to summarize business records and present those items in a condensed form).

5. Business and public records supported by a certificate are self-authenticating

The defendant did not challenge any of the business records certificates and previously indicated that he would stipulate to the authenticity of such records when supported by a certificate but has not agreed to the language in a proposed stipulation drafted by the government. *See* ECF No. 212. Thus, for avoidance of doubt, the government requests that the Court enter an order formally finding that the business and public records noticed in ECF No. 212 (or absence thereof) are self-authenticating and covered by exceptions to the rule against hearsay, including for business records (803(6)) and public records (803(8)). The government also anticipates filing a supplemental notice on November 24 based on new certificates that have been received since the previous notice.

PETER MCNEILLY
United States Attorney

s/ *Craig Fansler*
Craig Fansler
Sonia Dave
Assistant United States Attorneys
United States Attorney's Office
1801 California Street, Suite 1600
Denver, Colorado 80202
Telephone: (303) 454-0100
Craig.Fansler2@usdoj.gov
Sonia.Dave@usdoj.gov
Attorneys for the United States

CERTIFICATE OF SERVICE

I hereby certify that on November 21, 2025, I electronically filed the foregoing **GOVERNMENT'S TRIAL BRIEF** with the Clerk of the Court using the CM/ECF system which will send notification of such filing to counsel for the defendant.

s/ *Elizabeth Gomez Solis*
Elizabeth Gomez Solis
Legal Assistant
United States Attorney's Office