UNITED STATES DISTRICT COURT

for the

District of New Jersey

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

WEB-HOSTING ACCOUNTS AND ASSOCIATED DATA FOR WEBSITES FURTHER DESCRIBED IN ATTACHMENT A

Case No. 26-mj-8230

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the _____ District of New Jersey , there is now concealed *(identify the person or describe the property to be seized)*:

Instrumentalities of violations of and Property Forfeitable Title 18, United States Code, Section 981(a)(1)(A)

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☐ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18 USC Section 1956	Money Laundering

The application is based on these facts:

See Attachment C

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ [redacted]
Applicant's signature

[redacted], U.S. Postal Insecptor
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 11/05/2026

/s/ Jessica S. Allen/SN
Judge's signature

City and state: Newark, New Jersey

Hon. Jessica S. Allen, U.S.M.J.
Printed name and title

ATTACHMENT C

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF NEW JERSEY

IN THE MATTER OF THE SEIZURE OF WEB-HOSTING ACCOUNTS AND ASSOCIATED DATA FOR WEBSITES EJURORCOURTS.ORG, JUDICIALSERVICES.ORG, AND CIVILSERVICESDIVISION.ORG	)	Hon. Jessica S. Allen Mag. No.: 26 -8230 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEIZURE WARRANT

I, Postal Inspector [redacted], being duly sworn, hereby declare and state the following:

INTRODUCTION

1. I am a United States Postal Inspector with the United States Postal Inspection Service ("USPIS") and thus a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(c), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a seizure warrant.

2. I [redacted]

[redacted]

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. As set forth below, there is probable cause to believe that the web hosting accounts for domain names judicialservices.org, ejurorcourts.org, and civilservicesdivision.org (the "**TARGET WEB HOSTING ACCOUNTS"**) are property involved in, or traceable to property involved in a violation or violations of 18 U.S.C.§ 1956 (money laundering) (the "Specified Federal Offense"), and subject to seizure and forfeiture. I make this affidavit for a warrant to seize and restrain this property as described below in paragraphs 35-37.

BACKGROUND ON DOMAIN NAMES AND WEB HOSTING

5. Based on my training and experience and information learned from others, I am aware of the following:

6. Internet Protocol Address: An Internet Protocol address ("IP address") is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address: it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers ("ISPs"). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets ("octets") of numbers, each ranging from 0 to 255, separated by periods (e.g., 149.101.82.209). An IPv6 address has eight groups ("segments") of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (e.g., 2607:f330:5fa1:1020:0000:0000:0000:00d1).

7. Domain Name: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (e.g., "justice.gov"). Domain names are composed of one or more parts, or "labels," delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the "top-level domain" ("TLD") (e.g., ".com" or ".gov"). To the left of the TLD is the "second-level domain" ("SLD"), which is often thought of as the "name" of the domain. The SLD may be preceded by a "third-level domain," or "subdomain," which often provides additional information about various

functions of a server or delimits areas under the same domain. For example, in "www.justice.gov," the TLD is ".gov," the SLD is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

8. Domain Name System: The Domain Name System ("DNS") is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

9. Domain Name Servers: Domain Name Servers ("DNS servers") are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS "clients."

10. Registrar: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") or a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

11. Registry: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the ".com" and ".net" top-level domains is VeriSign, Inc., which is headquartered at 12061 Bluemont Way, Reston, Virginia.

12. Registrant: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically "point" their domain name to the IP address of the server where the registrant's website is hosted.

13. WHOIS: WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses, and related Internet resources. For example, results from a WHOIS search of a domain would likely include contact information for the registry, the registrar, and the ISP that owns the IP address to which the domain points. Contact information for the registrant of the domain might be provided but is often redacted, masked, or inaccurate.

14. Web hosting: A hosting provider, also referred to as a web hosting service or a web host, provides infrastructure to host websites and make them available on the internet.

PROBABLE CAUSE

Background on Jury Duty Fraud

15. The jury duty scam has plagued American victims for years, leading U.S. District, state and local courts to frequently warn the public about these scams.[1] According to the Federal Trade Commission's Consumer Sentinel Complaint

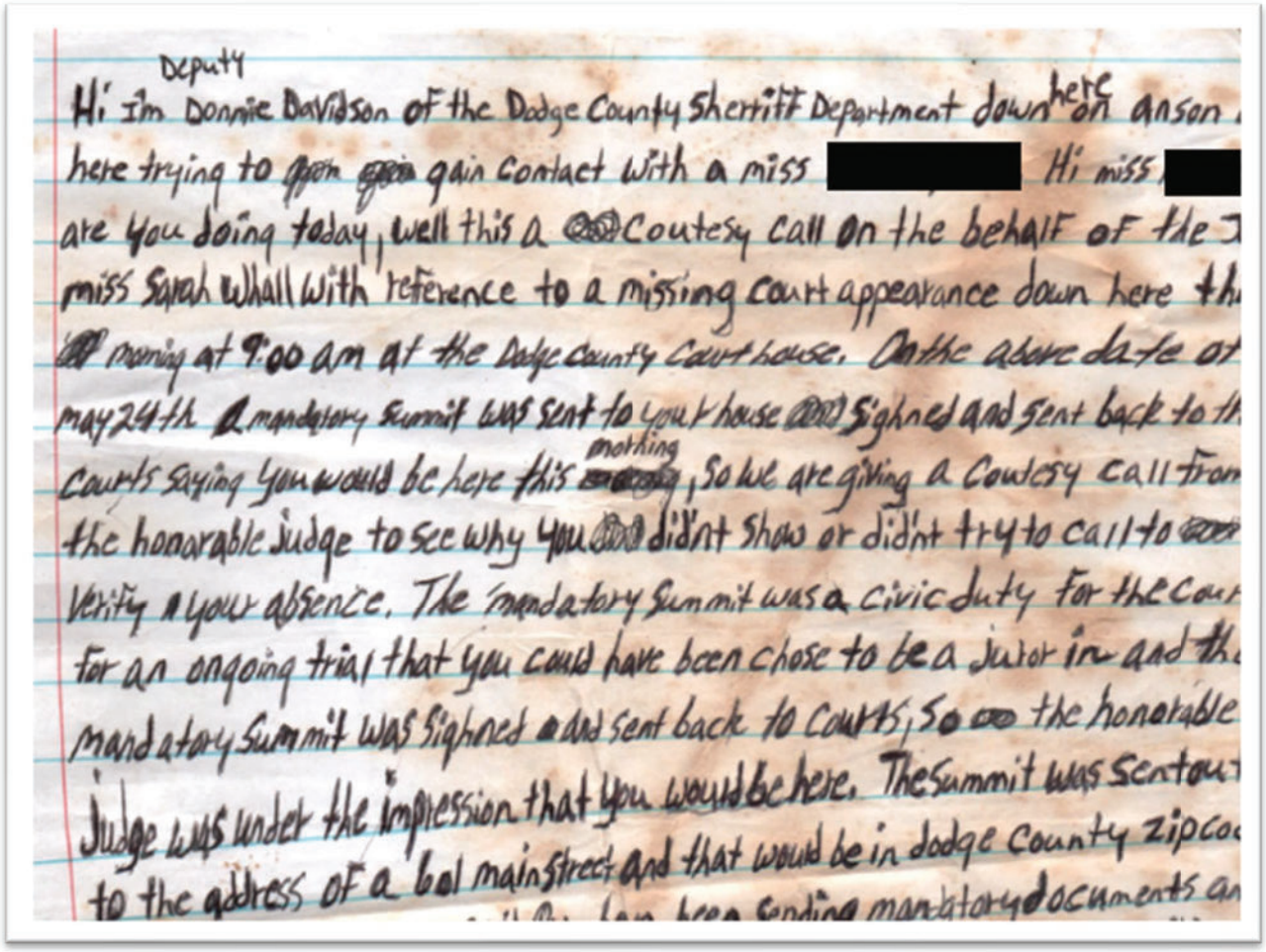
[1] Juror Scams, available at https://www.uscourts.gov/court-programs/jury-service/juror-scams (last accessed Oct. 28, 2026).

Database, from January 2021 through October 2026 there were over 30,000 complaints for jury duty impostor fraud, with consumers reporting losses exceeding $40 million. Recent complaint trends show that the scheme is an increasing threat to the public. In 2025, there were approximately 10,000 complaints with victims reporting $11m in losses. From January 2026 to October 2026, approximately 11,000 victims reported losses of around $13 million. Based on my training and experience, I believe victims of jury duty scams often incorrectly blame themselves and are too embarrassed or ashamed to report their victimization to law enforcement. Or they do not realize they have been defrauded. This results in widespread underreporting.

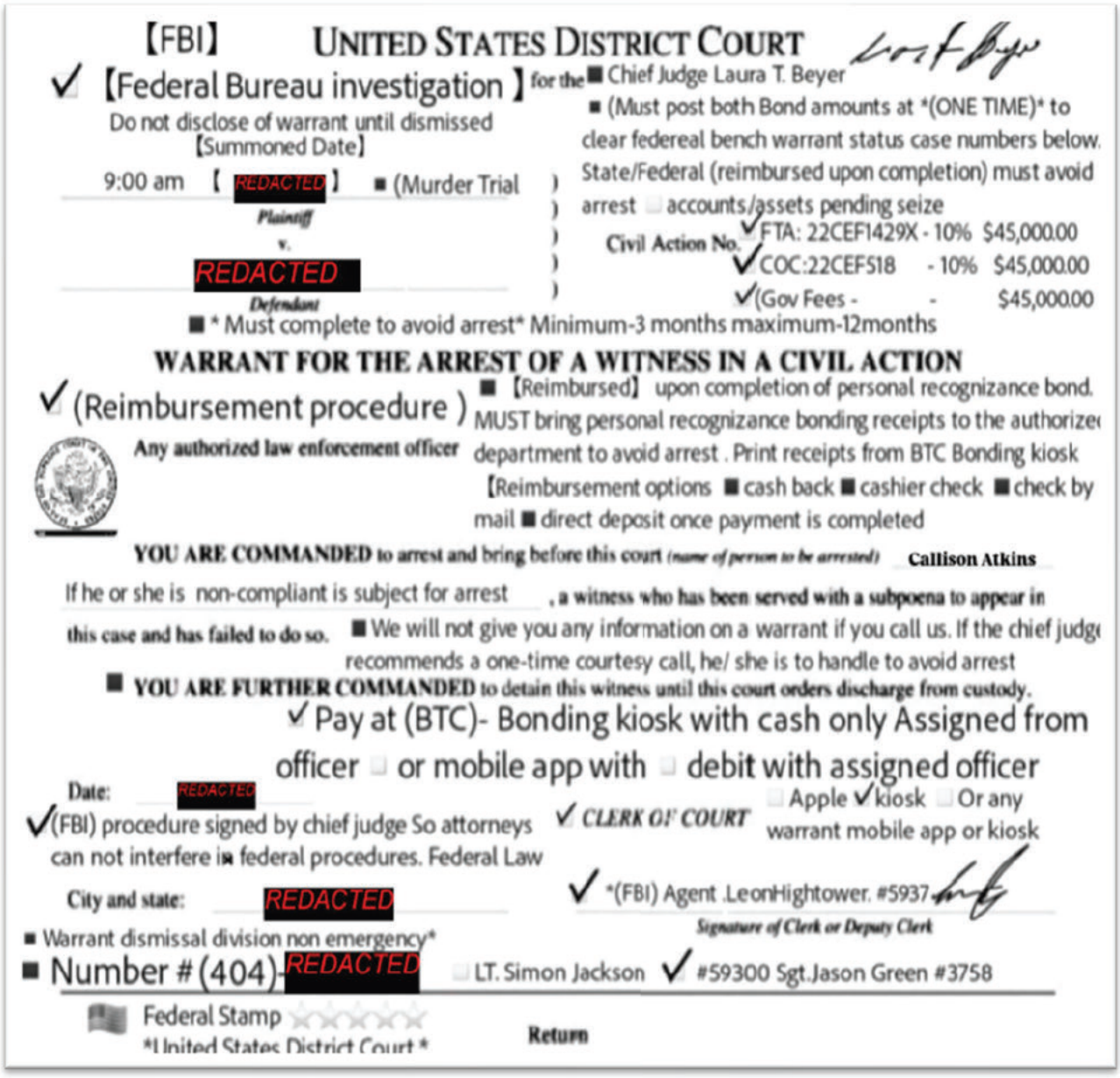
THE PHONE CALL

16. This scheme typically starts when a victim receives a telephone call in which their telephone's caller-ID identifies the caller as a local sheriff's department, the U.S. Marshals Service, or other law enforcement agency. When the victim picks up, the caller typically identifies themself as "officer [name]" and purported badge number. The "officer" claims that the victim failed to appear for jury duty and will be criminally charged, arrested and will go to jail. Oftentimes the caller claims that a warrant has been issued for their arrest. Scammers often follow scripts or skits, such as the hand-written script below when communicating with victims.

Figure 1 (below): a portion of a script used by an inmate for jury duty fraud scams. The script was obtained by the Georgia Department of Corrections ("GDC") during a search of the inmate's prison cell.


Deputy
Hi Im Donnie Davidson of the Dodge County Sheriff Department down here on Anson
here trying to gain contact with a miss [redacted] Hi miss
are you doing today, well this a courtesy call on the behalf of the J
miss Sarah Whall with reference to a missing court appearance down here th
morning at 9:00 am at the Dodge county court house. On the above date of
may 24th a mandatory summit was sent to your house signed and sent back to th
courts saying you would be here this morning, so we are giving a courtesy call from
the honorable Judge to see why you didnt show or didnt try to call to
verify your absence. The mandatory summit was a civic duty for the cou
for an ongoing trial that you could have been chose to be a juror in and th
mandatory summit was signed and sent back to courts, so the honorable
Judge was under the impression that you would be here. The summit was sent ou
to the address of a bol main street and that would be in dodge county zipco
sending mandatory documents a

17. Scammers frequently email or text victims counterfeit arrest warrants, and other official-looking documents including those pictured below in Figures 2 and 3. Scammers send these documents to dupe victims into believing that the scammers' bogus threats for missing jury duty are real.



【FBI】 UNITED STATES DISTRICT COURT

✓【Federal Bureau investigation】 for the ■ Chief Judge Laura T. Beyer

Do not disclose of warrant until dismissed

【Summoned Date】

9:00 am 【 REDACTED 】 ■ (Murder Trial

■ (Must post both Bond amounts at *(ONE TIME)* to clear federeal bench warrant status case numbers below. State/Federal (reimbursed upon completion) must avoid arrest ☐ accounts/assets pending seize

Plaintiff

v.

REDACTED

Defendant

Civil Action No.

✓FTA: 22CEF1429X - 10% $45,000.00

✓COC:22CEF518 - 10% $45,000.00

✓(Gov Fees - - $45,000.00

■ * Must complete to avoid arrest* Minimum-3 months maximum-12months

WARRANT FOR THE ARREST OF A WITNESS IN A CIVIL ACTION

✓(Reimbursement procedure) ■ 【Reimbursed】 upon completion of personal recognizance bond. MUST bring personal recognizance bonding receipts to the authorize department to avoid arrest . Print receipts from BTC Bonding kiosk 【Reimbursement options ■ cash back ■ cashier check ■ check by mail ■ direct deposit once payment is completed

Any authorized law enforcement officer

YOU ARE COMMANDED to arrest and bring before this court *(name of person to be arrested)* **Callison Atkins**

If he or she is non-compliant is subject for arrest , a witness who has been served with a subpoena to appear in this case and has failed to do so. ■ We will not give you any information on a warrant if you call us. If the chief judge recommends a one-time courtesy call, he/ she is to handle to avoid arrest

■ **YOU ARE FURTHER COMMANDED** to detain this witness until this court orders discharge from custody.

✓ Pay at (BTC)- Bonding kiosk with cash only Assigned from officer ☐ or mobile app with ☐ debit with assigned officer

Date: REDACTED

✓(FBI) procedure signed by chief judge So attorneys can not interfere in federal procedures. Federal Law

✓ *CLERK OF COURT*

☐ Apple ✓kiosk ☐ Or any warrant mobile app or kiosk

City and state: REDACTED

✓ *(FBI) Agent .LeonHightower. #5937

Signature of Clerk or Deputy Clerk

■ Warrant dismissal division non emergency*

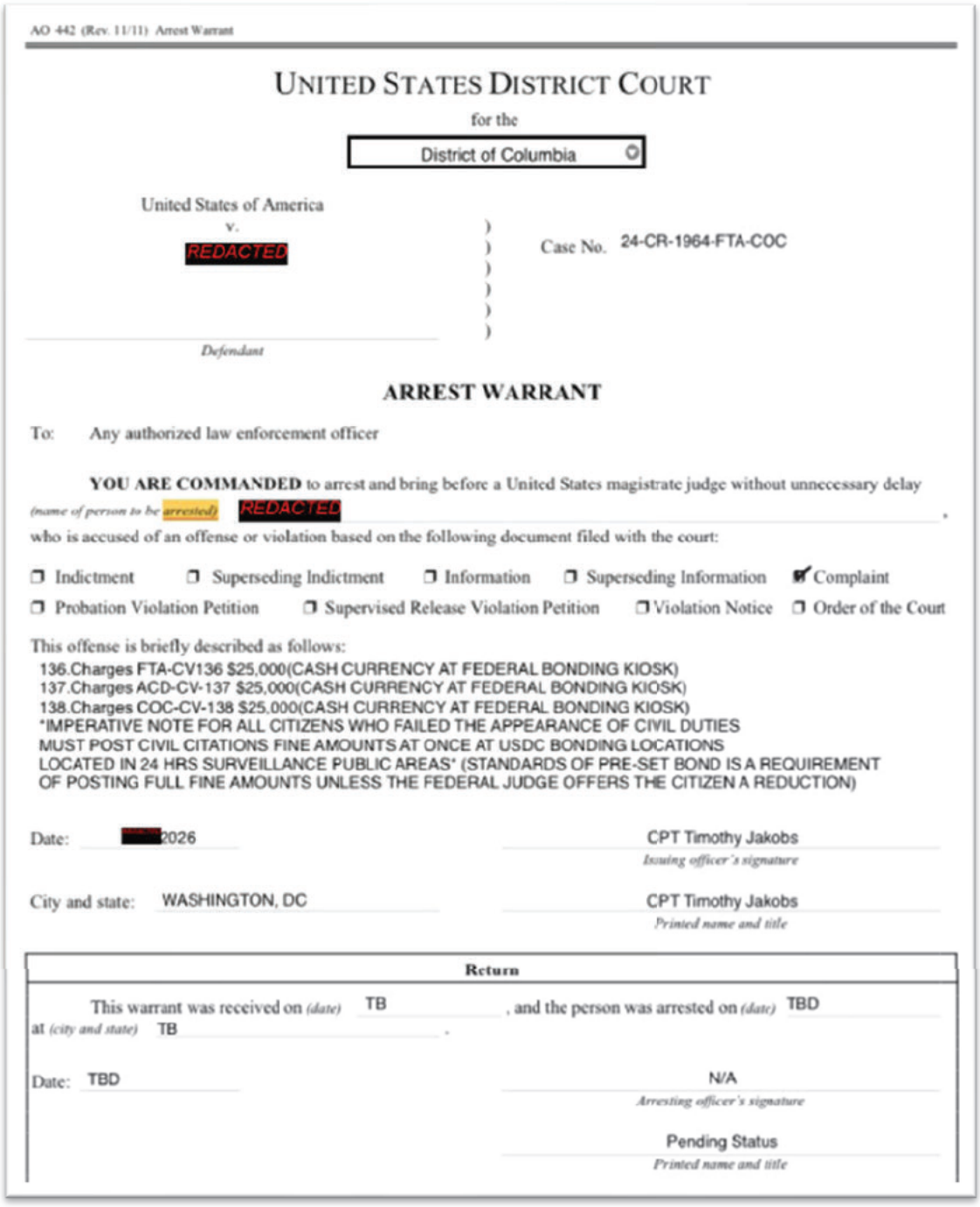
■ Number # (404)-REDACTED ☐ LT. Simon Jackson ✓ #59300 Sgt.Jason Green #3758

Federal Stamp

*United States District Court *

Return

Figure 2 — An example "arrest warrant" sent to a victim in 2025. This document was obtained pursuant to a lawfully executed search warrant in a jury duty fraud investigation. [redacted] *This document and others featured in this affidavit have been redacted to protect victims' privacy. The document includes the name of the "chief judge" Laura T. Beyer, who* ***is*** *the Chief Judge of the United States Bankruptcy Court in the Northern District of North Carolina. The document also commands the victim to make a payment at a "bonding" kiosk with cash.*



AO 442 (Rev. 11/11) Arrest Warrant

UNITED STATES DISTRICT COURT

for the

District of Columbia

United States of America
v.
REDACTED

Case No. 24-CR-1964-FTA-COC

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) REDACTED

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:

136.Charges FTA-CV136 $25,000(CASH CURRENCY AT FEDERAL BONDING KIOSK)
137.Charges ACD-CV-137 $25,000(CASH CURRENCY AT FEDERAL BONDING KIOSK)
138.Charges COC-CV-138 $25,000(CASH CURRENCY AT FEDERAL BONDING KIOSK)
*IMPERATIVE NOTE FOR ALL CITIZENS WHO FAILED THE APPEARANCE OF CIVIL DUTIES
MUST POST CIVIL CITATIONS FINE AMOUNTS AT ONCE AT USDC BONDING LOCATIONS
LOCATED IN 24 HRS SURVEILLANCE PUBLIC AREAS* (STANDARDS OF PRE-SET BOND IS A REQUIREMENT
OF POSTING FULL FINE AMOUNTS UNLESS THE FEDERAL JUDGE OFFERS THE CITIZEN A REDUCTION)

Date: [redacted]2026

CPT Timothy Jakobs
Issuing officer's signature

City and state: WASHINGTON, DC

CPT Timothy Jakobs
Printed name and title

Return

This warrant was received on *(date)* TB, and the person was arrested on *(date)* TBD

at *(city and state)* TB

Date: TBD

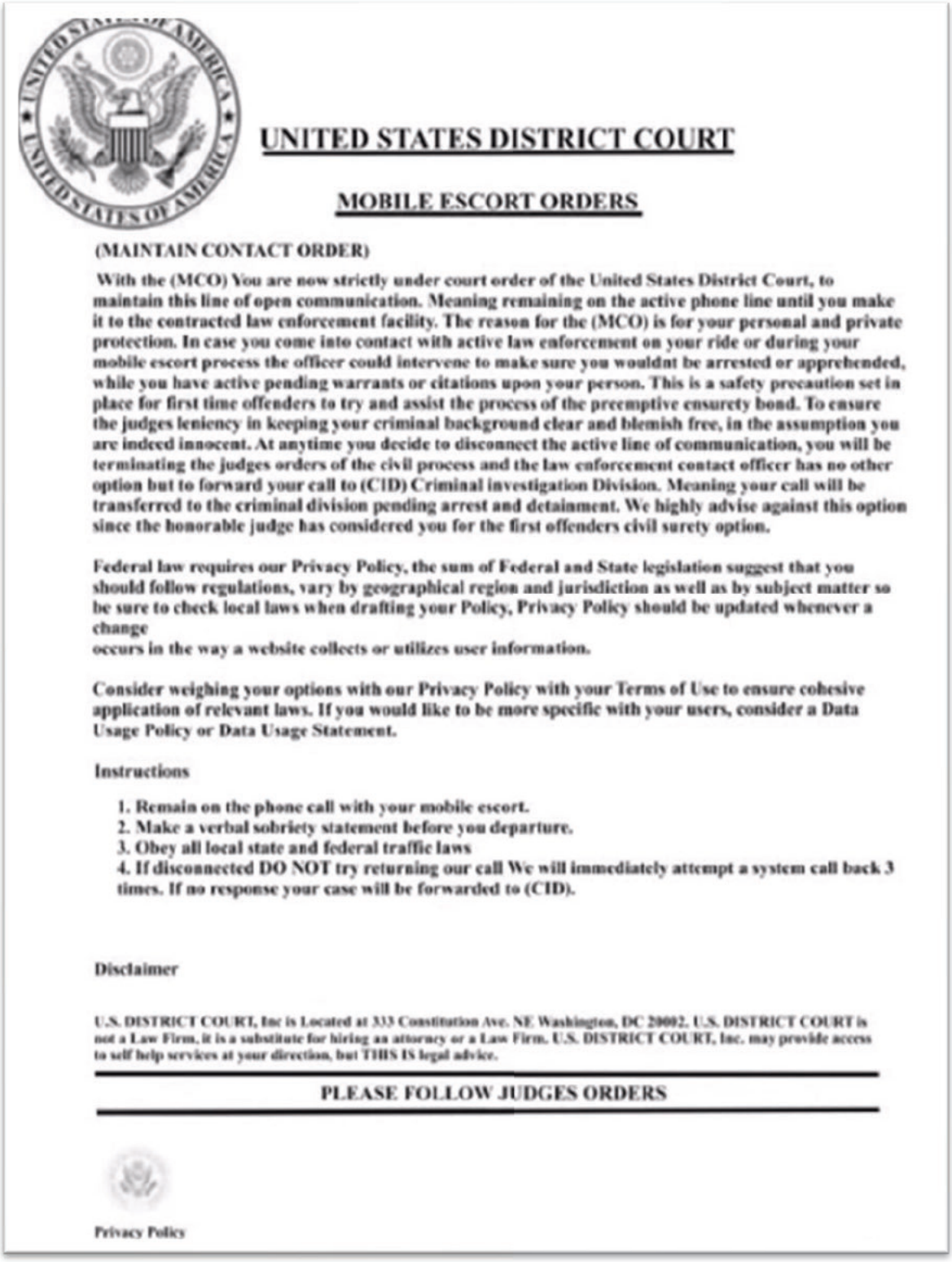
N/A
Arresting officer's signature

Pending Status
Printed name and title

Figure 3 — A second example "arrest warrant" sent to a victim in 2026. This document was obtained pursuant to a lawfully executed search warrant in a jury duty fraud investigation. [redacted] *The document appears to use the actual template form, AO 442, publicly available on the uscourts.gov website, and similar to Figure 2., appears to reference the need for the victim to make a payment at a federal*

bonding kiosk, a process used by the scammers to collect victim payments, further explained below.

Scammers employ social engineering techniques to intimidate victims and maintain a heightened sense of urgency all while preventing others from alerting the victim that they are being defrauded. For example, scammers typically instruct victims to remain on the phone until the process is resolved, under the guise that victims are being monitored by law enforcement and must remain in constant contact or else they could be subject to arrest. Scammers falsely claim that the victim is subject to a gag order, or a non-disclosure order, and are prohibited from telling anyone about the alleged proceedings against them. Both of these tactics are designed to cause physical and emotional stress on victims and prevent them engaging with friends or family who could cause them to question the threats and claims of the scammers. Victims have reported phone calls lasting over one day with jury duty fraudsters. The scammers will send additional bogus documents bolstering these instructions, such as the documents below.



UNITED STATES DISTRICT COURT

MOBILE ESCORT ORDERS

(MAINTAIN CONTACT ORDER)

With the (MCO) You are now strictly under court order of the United States District Court, to maintain this line of open communication. Meaning remaining on the active phone line until you make it to the contracted law enforcement facility. The reason for the (MCO) is for your personal and private protection. In case you come into contact with active law enforcement on your ride or during your mobile escort process the officer could intervene to make sure you wouldnt be arrested or apprehended, while you have active pending warrants or citations upon your person. This is a safety precaution set in place for first time offenders to try and assist the process of the preemptive ensurety bond. To ensure the judges leniency in keeping your criminal background clear and blemish free, in the assumption you are indeed innocent. At anytime you decide to disconnect the active line of communication, you will be terminating the judges orders of the civil process and the law enforcement contact officer has no other option but to forward your call to (CID) Criminal investigation Division. Meaning your call will be transferred to the criminal division pending arrest and detainment. We highly advise against this option since the honorable judge has considered you for the first offenders civil surety option.

Federal law requires our Privacy Policy, the sum of Federal and State legislation suggest that you should follow regulations, vary by geographical region and jurisdiction as well as by subject matter so be sure to check local laws when drafting your Policy, Privacy Policy should be updated whenever a change
occurs in the way a website collects or utilizes user information.

Consider weighing your options with our Privacy Policy with your Terms of Use to ensure cohesive application of relevant laws. If you would like to be more specific with your users, consider a Data Usage Policy or Data Usage Statement.

Instructions

1. **Remain on the phone call with your mobile escort.**
2. **Make a verbal sobriety statement before you departure.**
3. **Obey all local state and federal traffic laws**
4. **If disconnected DO NOT try returning our call We will immediately attempt a system call back 3 times. If no response your case will be forwarded to (CID).**

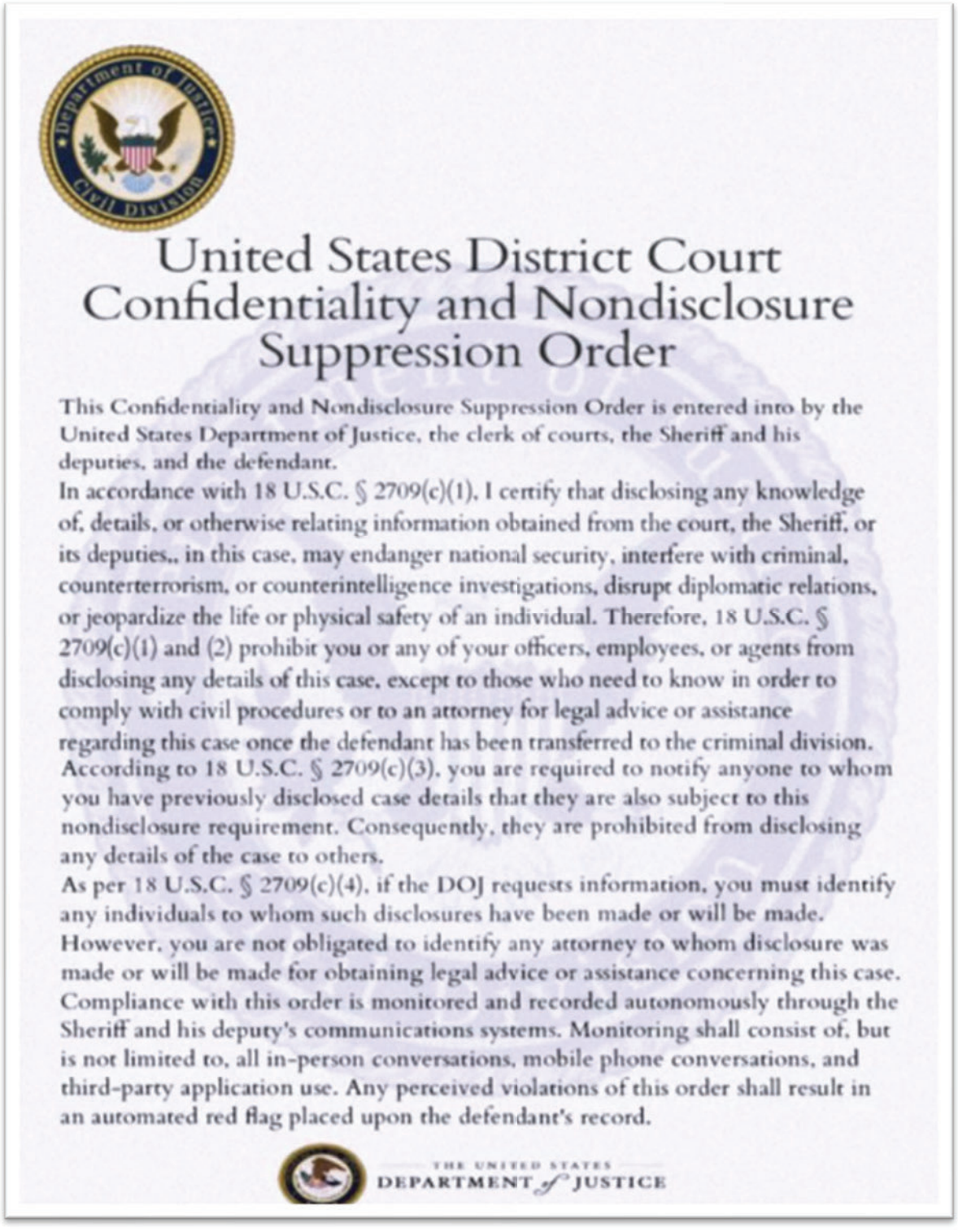
Disclaimer

U.S. DISTRICT COURT, Inc is Located at 333 Constitution Ave. NE Washington, DC 20002. U.S. DISTRICT COURT is not a Law Firm, it is a substitute for hiring an attorney or a Law Firm. U.S. DISTRICT COURT, Inc. may provide access to self help services at your direction, but THIS IS legal advice.

PLEASE FOLLOW JUDGES ORDERS

Privacy Policy

Figure 4 — a document emailed to victims [redacted]. The document bears official seals of the United States and directs the victim to "remain on the phone call."



United States District Court
Confidentiality and Nondisclosure Suppression Order

This Confidentiality and Nondisclosure Suppression Order is entered into by the United States Department of Justice, the clerk of courts, the Sheriff and his deputies, and the defendant.

In accordance with 18 U.S.C. § 2709(c)(1), I certify that disclosing any knowledge of, details, or otherwise relating information obtained from the court, the Sheriff, or its deputies,, in this case, may endanger national security, interfere with criminal, counterterrorism, or counterintelligence investigations, disrupt diplomatic relations, or jeopardize the life or physical safety of an individual. Therefore, 18 U.S.C. § 2709(c)(1) and (2) prohibit you or any of your officers, employees, or agents from disclosing any details of this case, except to those who need to know in order to comply with civil procedures or to an attorney for legal advice or assistance regarding this case once the defendant has been transferred to the criminal division.

According to 18 U.S.C. § 2709(c)(3), you are required to notify anyone to whom you have previously disclosed case details that they are also subject to this nondisclosure requirement. Consequently, they are prohibited from disclosing any details of the case to others.

As per 18 U.S.C. § 2709(c)(4), if the DOJ requests information, you must identify any individuals to whom such disclosures have been made or will be made. However, you are not obligated to identify any attorney to whom disclosure was made or will be made for obtaining legal advice or assistance concerning this case.

Compliance with this order is monitored and recorded autonomously through the Sheriff and his deputy's communications systems. Monitoring shall consist of, but is not limited to, all in-person conversations, mobile phone conversations, and third-party application use. Any perceived violations of this order shall result in an automated red flag placed upon the defendant's record.

THE UNITED STATES DEPARTMENT of JUSTICE

Figure 5 — a document emailed to victims with instructions to not to "disclos[e] any knowledge of, details or otherwise relating information from the court, the Sheriff . . ." The document bears the official seal of the Justice Department. [redacted]

IMPOSTOR WEBSITES

18. At times, jury duty scammers use official looking websites, such as the **TARGET WEB HOSTING ACCOUNTS**, that impersonate actual government websites, such as the United States Courts website uscourts.gov. Victims are often instructed to input personal identifiable information ("PII") into these sites, such as a picture of their driver's license and their social security number. The websites at times display information about the victim's court appearance for missing jury duty, and fines that the victim needs to pay to avoid arrest. Scammers direct victims to these sites to add credibility to their claims that they are actual law enforcement and that there is a real proceeding against the victim for missing jury duty. As described further below, this affidavit is submitted in support of seizure of websites used in furtherance of jury duty impostor schemes.

THE PAYMENT

19. After frightening and convincing victims that they will be arrested if they fail to comply with their instructions, scammers typically offer victims a chance to resolve the alleged legal process by making a payment. This payment is sometimes referred to as a "bond" payment which scammers falsely promise to return to the victim after they comply with their demands. Victims, fearing arrest and other consequences, typically pay the scammers thousands of dollars, with some victims paying hundreds of thousands of dollars. At times, particularly vulnerable victims that make an initial payment are convinced by the scammers through additional lies that they owe more money. At times, scammers convince victims to apply for and

obtain personal loans to finance payments. Some victims have filed for bankruptcy after defaulting on loans they received to finance jury duty fraud payments. Other victims report losing their life savings and having suicidal thoughts.

20. Jury duty scammers frequently direct victims to pay via cryptocurrency ATMs ("crypto ATMs"). Cryptocurrency ("crypto"), such as bitcoin, is a pseudonymous virtual currency that secures transactions using complicated encryption methods and operates outside of the traditional financial system. Crypto ATMs are physical kiosks allowing users to send cryptocurrency payments by depositing cash.

21. Crypto ATMs function similar to traditional bank ATMs. To use a Crypto ATM platform, such as Bitcoin Depot, Bitstop or Coinhub, users typically submit know your customer information "KYC," such as their name, address, telephone number, email, social security number, photos or videos of their likeness and a picture of their photo-id. Once approved, a customer can deposit cash into a crypto ATM, and after verifying their identity, typically by inputting an authentication code the crypto ATM platform texts to the customer's phone, send a crypto payment to a crypto address of their choice. The machine accepts the cash, charges a fee, and then converts the remaining amount to crypto at a quoted exchange rate. The crypto ATM platform then sends this crypto to the destination address inputted by the customer at the kiosk. For ease, customers typically scan a QR code at the kiosk which links to the crypto address they wish to send the deposited cash. The crypto ATM will often take a photo of the individual using the kiosk when they

complete the transaction; however, the kiosk user, assumed to be the account holder, is typically not required to provide any personally identifiable information at the kiosk, such as their name or address.

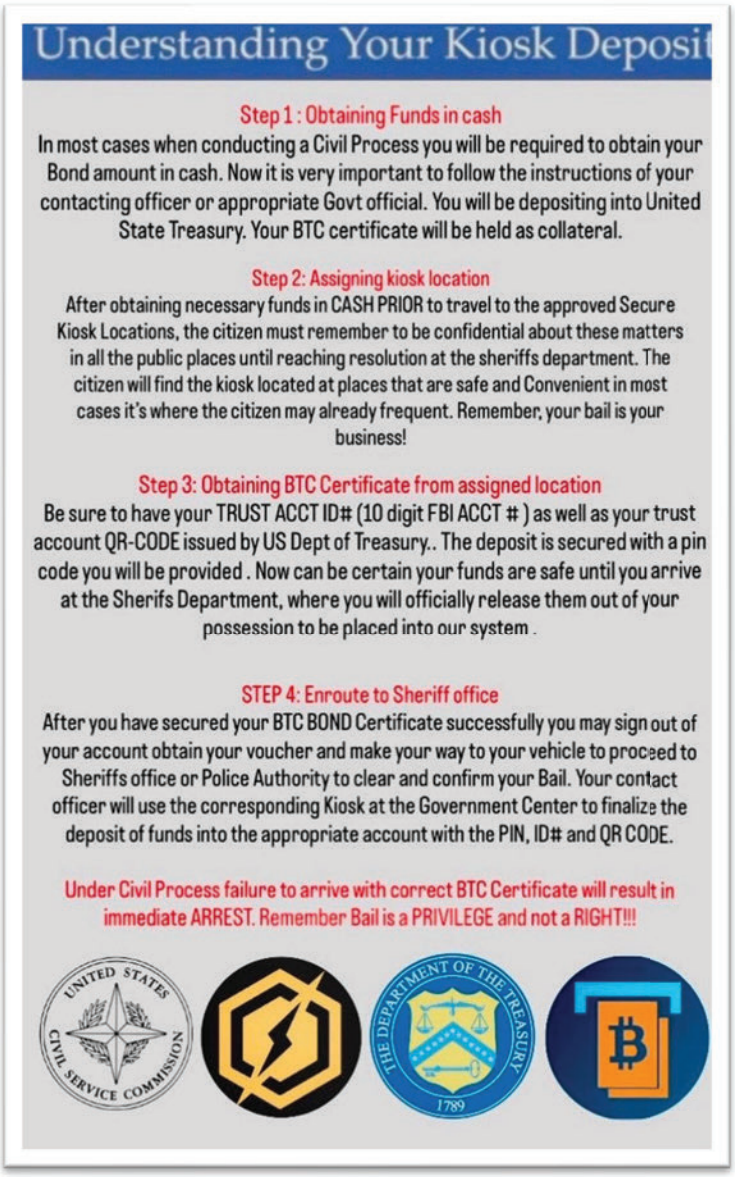
22. Jury duty scammers take advantage of crypto ATMs as a fast and anonymous method to obtain victim payments. The scammers direct victims to travel to their bank, withdraw cash, while either not informing any bank employee about the nature of the withdrawal or lie to the employee about the reason for the withdrawal to prevent them from intervening. After obtaining the cash, victims are instructed to travel to the nearest crypto ATM to deposit the cash to pay the alleged fine or "bond" for missing jury duty.

23. Scammers direct victims to input a phone number controlled by the scammer or by one of their accomplices into the crypto ATM. Typically, the crypto ATM platform then sends a text message to that phone to verify the identity of the individual using the kiosk at that moment. The scammers obtain this code and provide it to the victim to input into the kiosk. After doing so, the victim gains access to the platform and can now send their cash to almost any crypto address of their choosing. Scammers will then send QR codes to the victim, linked to crypto addresses under their control.



Figure 6 — a QR code and instructions texted to a jury duty fraud victim to scan at a crypto ATM. Similar to the counterfeit arrest warrant, Figure 2, the image references the same Chief Judge, Laura T. Beyer. This image was provided to government investigators by a jury duty fraud victim who lost more than $40,000.

24. The scammers also provide victims, often via emailed or texted official looking documents, detailed instructions regarding the purpose and procedure for paying via crypto ATM:



Understanding Your Kiosk Deposit

Step 1 : Obtaining Funds in cash

In most cases when conducting a Civil Process you will be required to obtain your Bond amount in cash. Now it is very important to follow the instructions of your contacting officer or appropriate Govt official. You will be depositing into United State Treasury. Your BTC certificate will be held as collateral.

Step 2: Assigning kiosk location

After obtaining necessary funds in CASH PRIOR to travel to the approved Secure Kiosk Locations, the citizen must remember to be confidential about these matters in all the public places until reaching resolution at the sheriffs department. The citizen will find the kiosk located at places that are safe and Convenient in most cases it's where the citizen may already frequent. Remember, your bail is your business!

Step 3: Obtaining BTC Certificate from assigned location

Be sure to have your TRUST ACCT ID# (10 digit FBI ACCT #) as well as your trust account QR-CODE issued by US Dept of Treasury.. The deposit is secured with a pin code you will be provided . Now can be certain your funds are safe until you arrive at the Sherifs Department, where you will officially release them out of your possession to be placed into our system .

STEP 4: Enroute to Sheriff office

After you have secured your BTC BOND Certificate successfully you may sign out of your account obtain your voucher and make your way to your vehicle to proceed to Sheriffs office or Police Authority to clear and confirm your Bail. Your contact officer will use the corresponding Kiosk at the Government Center to finalize the deposit of funds into the appropriate account with the PIN, ID# and QR CODE.

Under Civil Process failure to arrive with correct BTC Certificate will result in immediate ARREST. Remember Bail is a PRIVILEGE and not a RIGHT!!!

UNITED STATES CIVIL SERVICE COMMISSION

THE DEPARTMENT OF THE TREASURY 1789

Figure 7 — an official looking document emailed to a victim providing instructions on making a payment using a crypto ATM. The "TRUST ACCT ID," trust account QR-CODE, and pin code referenced in the document appear to be references to the phone number the victim inputs into the kiosk to enable the cash deposit, the QR code the

victim scans to send crypto, and the authentication code the victim inputs after the phone number they entered receives an authentication code from the crypto ATM platform. The document also contains official seals for two U.S. government agencies, as well as the company logos for two widely use crypto ATM platforms: Bitcoin Depot, featured on the bottom left of the document, between the treasury and civil service commission seals, and Coinhub, located on the bottom right. [redacted]

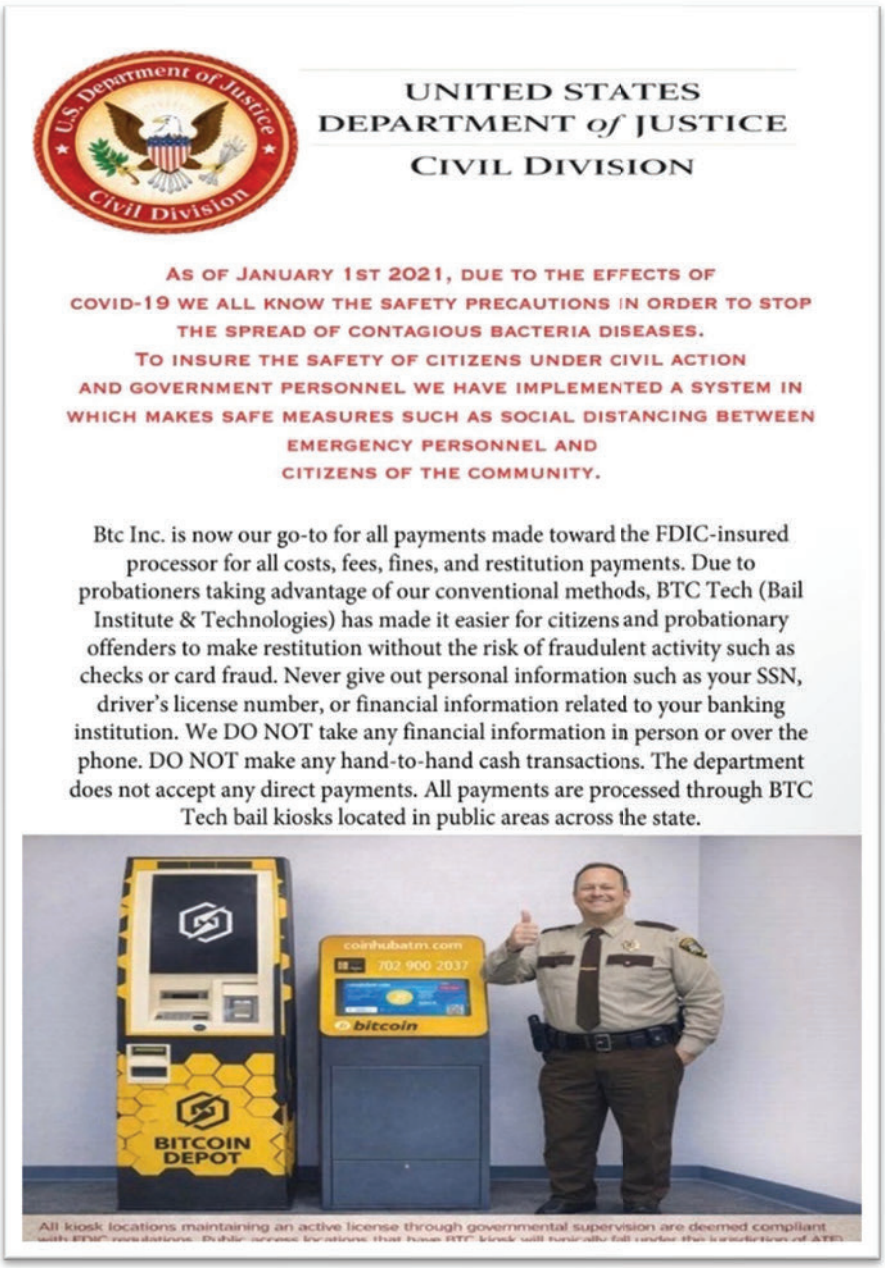
Victims then deposit their cash and complete the transaction:



Figure 8 — a crypto ATM photo of a victim using a kiosk. The victim is seen holding a stack of $100 bills while speaking on the phone with a jury duty scammer. [redacted] *The victim's likeness has been blurred to protect their privacy.*

25. By using crypto ATMs in this way, scammers conceal the nature of the transaction's source and destination from law enforcement and financial institutions, consistent with setting up the laundering of the funds, in violation of Title 18, United States Code, Section 1956(a)(1). Scammers falsely claim that crypto ATMs are the

verified and secure payment method accepted by courts. Scammers send victims bogus explanatory information, such as the flyer emailed to victims below, to convince victims that payment via crypto ATMs is a legitimate form of payment accepted by the U.S. government.



UNITED STATES
DEPARTMENT *of* JUSTICE
CIVIL DIVISION

AS OF JANUARY 1ST 2021, DUE TO THE EFFECTS OF COVID-19 WE ALL KNOW THE SAFETY PRECAUTIONS IN ORDER TO STOP THE SPREAD OF CONTAGIOUS BACTERIA DISEASES.
TO INSURE THE SAFETY OF CITIZENS UNDER CIVIL ACTION AND GOVERNMENT PERSONNEL WE HAVE IMPLEMENTED A SYSTEM IN WHICH MAKES SAFE MEASURES SUCH AS SOCIAL DISTANCING BETWEEN EMERGENCY PERSONNEL AND CITIZENS OF THE COMMUNITY.

Btc Inc. is now our go-to for all payments made toward the FDIC-insured processor for all costs, fees, fines, and restitution payments. Due to probationers taking advantage of our conventional methods, BTC Tech (Bail Institute & Technologies) has made it easier for citizens and probationary offenders to make restitution without the risk of fraudulent activity such as checks or card fraud. Never give out personal information such as your SSN, driver's license number, or financial information related to your banking institution. We DO NOT take any financial information in person or over the phone. DO NOT make any hand-to-hand cash transactions. The department does not accept any direct payments. All payments are processed through BTC Tech bail kiosks located in public areas across the state.

All kiosk locations maintaining an active license through governmental supervision are deemed compliant

Figure 9 — a document emailed to a victim, purporting to be from the US Department of Justice's Civil Division, picturing a sheriff endorsing crypto ATMs as an official form of payment. [redacted]

26. Scammers typically route victim payments through a series of intermediaries, for the purposes of disguising and concealing the illicit nature of the payment. For example, figure 10 below displays how one jury duty victim crypto ATM deposit, the left-most icon, was transmitted through multiple crypto addresses, before reaching destination addresses presumed to be associated with the scammer (the rightmost circles). As indicated by the send dates below the flow arrows, the payments are quickly moved from one crypto address to another before reaching the final destination addresses.

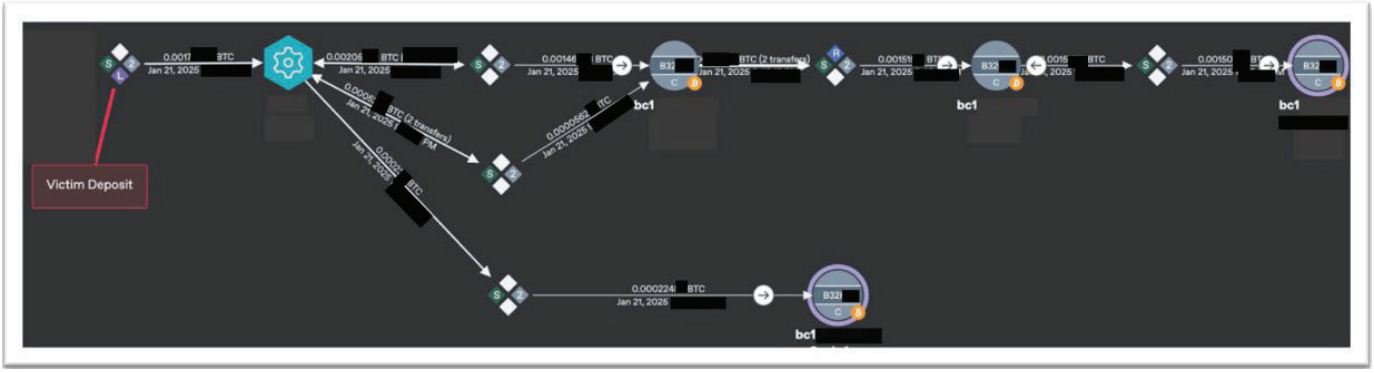


Figure 10 — An example crypto tracing graph created by investigators in a jury duty fraud investigation showing the flows of crypto funds from a victim deposit at a crypto ATM. The funds are routed between numerous crypto addresses, a portion of which is transferred to the rightmost addresses represented by the circles with purple rings.

Based on my training and experience, I believe that the rapid movement of victim funds derived from jury duty fraud through multiple accounts in quick succession is evidence of money laundering concealment, as indicated in title 18, United States Code, Section 1956(a)(1)(B)(i).

THE SCAMMERS

27. Based on evidence obtained from financial institutions, announced charges against jury duty scammers, and my experience, I believe that the vast majority of jury duty fraud perpetrators are incarcerated inmates within the Georgia state prison system. For example, in 2016, FBI's Operation Ghost Guard investigated widespread criminal activity and corruption within Georgia prisons committed by inmates, prison guards, and their co-conspirators. Among other illegal activity, Georgia prisoners used contraband cell phones smuggled into the prisons by correctional officers to perpetrate jury duty fraud schemes. The initiative led to the indictment of approximately 130 individuals.[2] Since 2016, law enforcement has charged and convicted numerous Georgia prisoners with jury duty scams, including a recent conviction of two inmates in 2026 for a scheme that defrauded at least 119 victims of over $464,000.[3]

---

[2] "Operation Ghost Guard Widespread Public Corruption inside Georgia Prisons" (Feb. 11, 2016), available at https://www.fbi.gov/news/stories/-operation-ghost-guard (last accessed Oct. 28. 2026).

[3] "Georgia Inmates Found Guilty in Nationwide Jury Duty Call Scheme" (Jan. 9, 2026), available at https://www.justice.gov/usao-mdga/pr/georgia-inmates-found-guilty-nationwide-jury-duty-call-scheme (last accessed Oct. 27, 2026).

See also, e.g., "Further Corruption Involving Georgia Department of Corrections Guards Exposed" (Feb. 11, 2016), available at https://www.justice.gov/usao-ndga/pr/further-corruption-involving-georgia-department-corrections-guards-exposed (last accessed Oct. 28, 2026); highlighting multiple indictment of 49 Georgia correctional officers with smuggling contraband into prisons.

See also, e.g., "Former Prison Inmate from Georgia Sentenced for Defrauding Victims Out of Over $9,700" (June 10, 2022), available at https://www.justice.gov/usao-

28. Victims frequently complain to crypto ATM platforms after they have been defrauded in jury duty fraud schemes. Victims ask these companies to stop the transmission of their crypto transactions only to be told that the transactions are irreversible and final. Information from these complaints show the proliferation of Georgia money mules facilitating jury duty scams. Based on my experience and

---

wdla/pr/former-prison-inmate-georgia-sentenced-defrauding-victims-out-over-9700 (last accessed Oct. 28, 2026); Reese, a Georgia state prison inmate at Jimmy Autry State Prison, participated in a jury duty fraud scheme using contraband cell phones to contact victims.

See also, e.g., "Georgia Inmate Pleads Guilty to Conspiracy to Commit Wire Fraud for His Role in Grand Jury Scam" (June 13, 2019), available at https://www.justice.gov/usao-edla/pr/georgia-inmate-pleads-guilty-conspiracy-commit-wire-fraud-his-role-grand-jury-scam (last accessed Oct. 28, 2026); Allen, also an inmate at Jimmy Autry State Prison, participated in a jury duty fraud scheme using a contraband cell phone and collected $5,500 from at least one victim.

See also, e.g., "Georgia inmate sentenced for running a multi-million-dollar fraud scheme from state prison" (Dec. 1, 2021) available at https://www.justice.gov/usao-ndga/pr/georgia-inmate-sentenced-running-multi-million-dollar-fraud-scheme-state-prison (last accessed Oct. 28, 2026) – A GDC inmate operated a scheme involving the theft of nearly $3 million in heavy equipment from various dealers using contraband cell phones.

See also, e.g., "Atlanta man indicted for stealing $11 million while in prison" (Dec. 10, 2020) available at https://www.justice.gov/usao-ndga/pr/utah-resident-indicted-operating-fake-charities-falsely-claimed-donations-would-benefit (last accessed Oct. 28, 2026) – A Georgia prison inmate was convicted of conspiracy to commit bank fraud and money laundering in connection with the theft of approximately $11 million from a Charles Schwab account using a contraband cell phone.

See also, e.g., United States v. Asaad Amir Hasuan (2024) – A Georgia inmate allegedly obtained more than $3.5 million through schemes targeting other inmates' family members and friends, including false promises of legal assistance, protection, and investment opportunities.

evidence I have reviewed in jury duty scam investigations, I believe that most inmates in Georgia prisons will use friends and family members, the majority of whom reside in Georgia, to accept and forward victim payments. Thus, a money mule's state of residence is highly probative of the location of the jury duty scammer.

29. For example, records obtained from Bitcoin Depot, formerly one of the nation's largest crypto ATM companies[4], show that between September 2022 and May 2026 victims reported losing over $19m in jury duty fraud schemes. Among these complainants over 40% made payments to money mules located in Georgia. Approximately 20 victims made payments to current or former Georgia inmates or their suspected family members.

How Jury Duty Scammers Acquire Contraband to Perpetrate the Scheme

30. Media outlets have extensively reported illicit activity within Georgia prisons for years. A number of Georgia state prisons are essentially serving as domestic scam compounds and criminal epicenters perpetrating jury duty fraud and other crimes victimizing the American public. Georgia inmates bribe prison employees and use drones to smuggle contraband cell phones, cash, drugs and other illicit items into prisons.

[4] Bitcoin Depot filed for Chapter 11 bankruptcy on May 18, 2026. *See* https://finance.yahoo.com/markets/crypto/articles/crypto-atm-operator-bitcoin-depot-093609055.html; accessed Oct. 13, 2026.

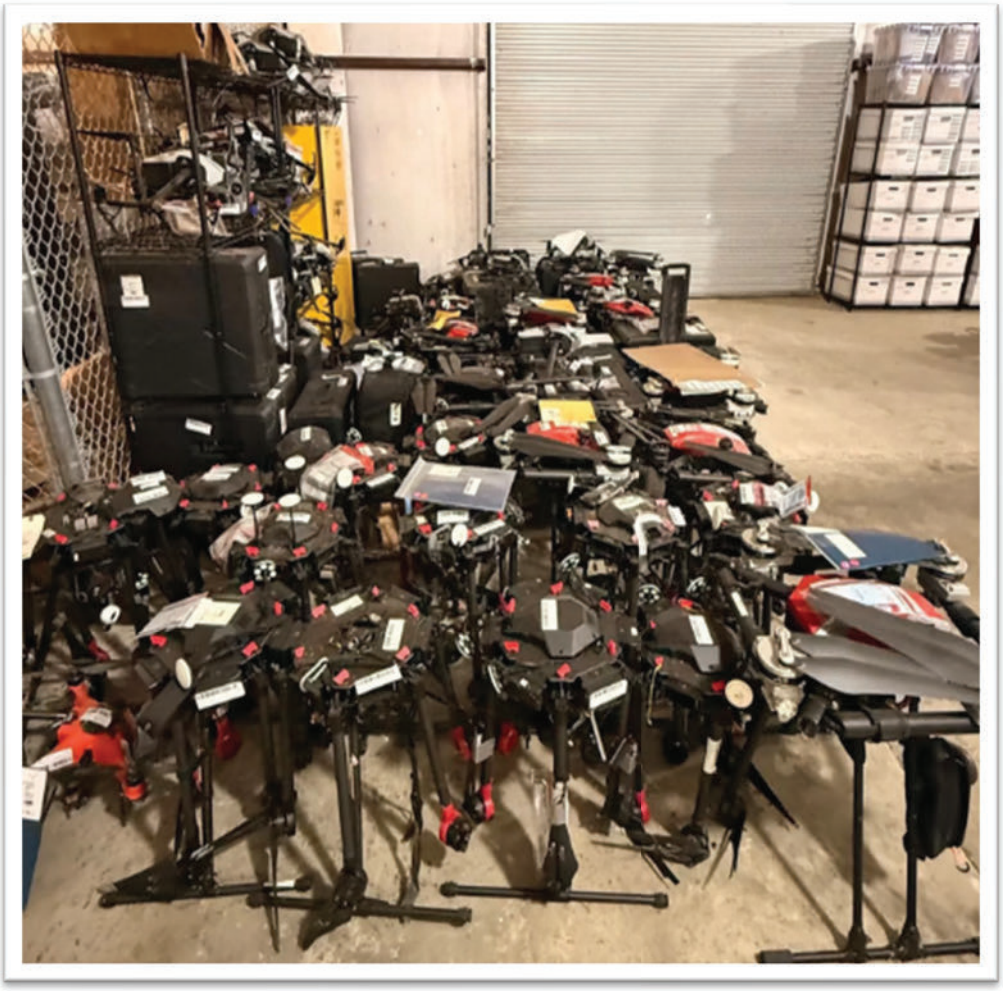


Figure 11 — a warehouse with drones seized by Georgia Department of Corrections (GDC). These drones were used to transport illicit items, including cell phones and cash to state prisons. See "'Threat from above': Prisons face escalating threat from drones" (Dec. 12, 2025), available at: https://abcnews.com/US/threat-prisons-face-escalating-threat-drones/story?id=128243809 (last accessed Oct. 30, 2026).



Figure 12 – a photo of a drone transporting contraband into a prison taken by GDC. Id.

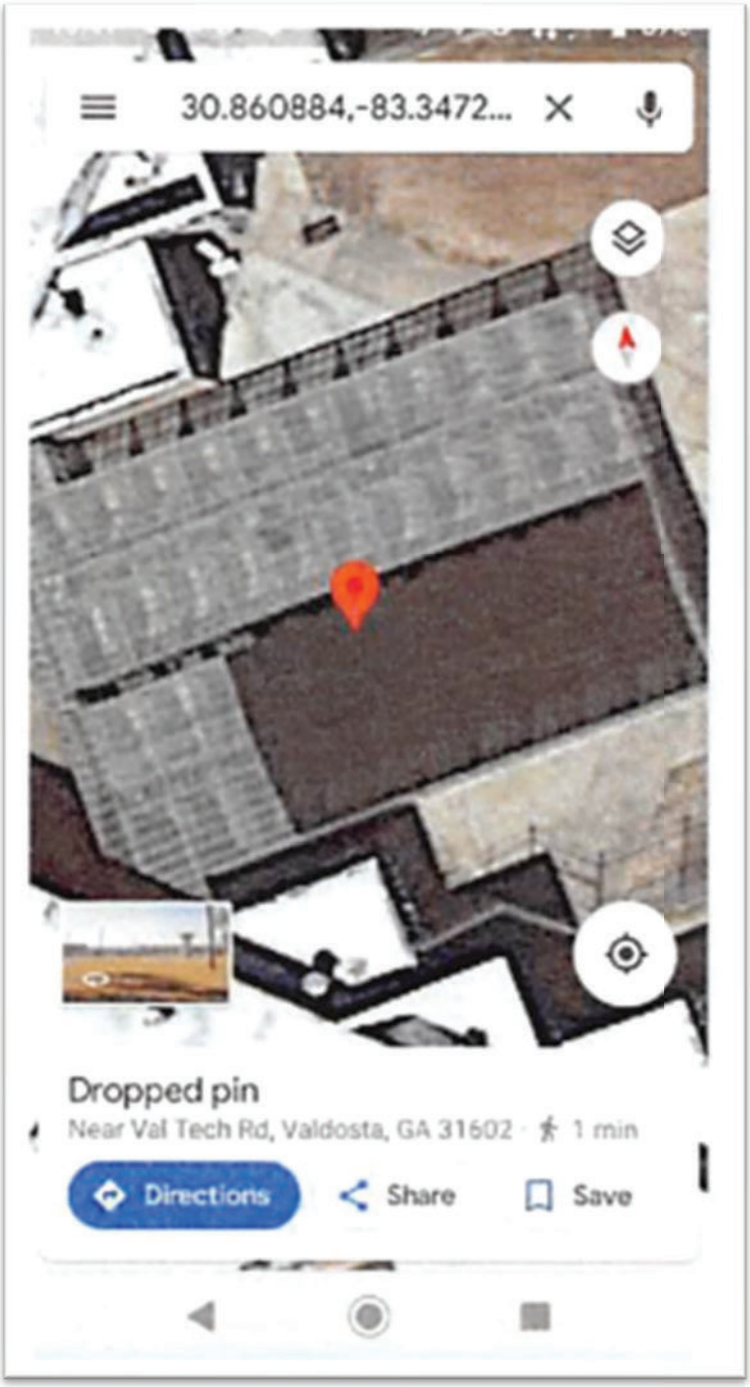


Figure 13 — a mobile phone screenshot showing a Google Map's location within Valdosta state prison, taken by a defendant in United States v. Hall. In Hall, 16 defendants were charged with conspiring to distribute marijuana and methamphetamine by using drones. The defendants orchestrated a scheme to fly drones into numerous state prisons to deliver drugs, cell phones and other contraband items from at least 2019 through July 2024. The photo shows inmates providing their coordinates to drone operators to facilitate contraband delivery. See Indictment at 68,

United States v. Hall et al., *No. 24-CR-00009 (S.D. Ga., 2024), https://www.justice.gov/usao-sdga/media/1364706/dl?inline.*



Figure 14 –a picture taken by a defendant in Hall, showing contraband organized for a drone delivery which includes mobile phones and illicit drugs. Id. at 53.

31. From 2018 to 2023, at least 360 GDC employees were arrested for smuggling contraband into state prisons. High profile cases include 2019 charges against a lieutenant at Hays State Prison who smuggled drugs for a convicted murderer. The officer quipped that the inmate she was smuggling contraband for

was "trying to have me doing fed time, like for real." She further stated that she would need to "wrap [the drugs] . . . so I'm sure ain't nothing smelling."[5]

32. In perhaps the most egregious example, a warden of Smith State prison, Brian Adams, was charged by state authorities in May 2026 with RICO, bribery, and false statements among other crimes. Adams allegedly received cash for smuggling contraband and assisted an inmate, Nathan Weekes, who had been convicted of armed robbery. In addition to smuggling contraband and providing preferential treatment to Weekes, prosecutors alleged that Adams concealed prison shanks and contraband cell phones by having them buried in his backyard to obstruct the police investigation.[6] Weekes and his associates were also charged with orchestrating a murder for hire plot, planning to kill a Smith State prison guard at the guard's home in Glennville, Georgia, where the prison is located. Weekes's accomplices mistakenly entered the wrong residence and murdered an innocent elderly veteran.

33. After acquiring contraband phones, scammers have all the means necessary to perpetrate the scheme. They use publicly available applications like "true people finder" to locate potential victims; they use mobile applications to obtain temporary, burner, phone numbers to contact victims; and they use caller-id spoofing

[5] *See* Georgia Prison Corruption, (Sept. 21, 2023) (https://www.ajc.com/sp/news/investigations/prisons-inside-job) (last accessed Oct. 8, 2026).

[6] See *State of Georgia v. Brian Dennis Adams*, (2026-R-107, Superior Court of Tattnall County, May 2026). Available at: https://law.georgia.gov/press-releases/2026-05-13/carr-indicts-former-prison-warden-contraband-smuggling-operation.

applications. With these spoofing applications, scammers' outbound calls to victims can appear as if they originated from actual law enforcement numbers, such as a local sheriff's office. The scammers also use their phones to create everything they need to collect victim payments, including email accounts, cryptocurrency exchange accounts, and crypto ATM accounts. They use phones to communicate with other inmates and their accomplices outside prison walls. After they obtain victim funds, scammers send money to relatives and friends, purchase expensive jewelry or drugs, or simply have a drone or prison guard smuggle their cash directly into the prison.

Flaunting the scam

34. Scammers are frequently members of national organized gangs, such as the Bloods and Gangster Disciples, and are often serving lengthy sentences for violent crimes, including murder. Flaunting their ill-gotten gains is a form of social currency, increasing their personal notoriety within the gang and the prison. Despite taking numerous steps to hide their illicit activities from financial institutions and law enforcement, once they have their cash and contraband items, they often boast about their ability to victimize Americans and steal money. Scammers frequently post videos and photos to their social media accounts flaunting their contraband items and the fruits of their criminal activity.



Figure 15 — A Facebook post showing Georgia inmate flaunting cash while wearing what appears to be an expensive wristwatch.



Figure 16—a Facebook post showing a Georgia inmate posing with four cellular telephones.

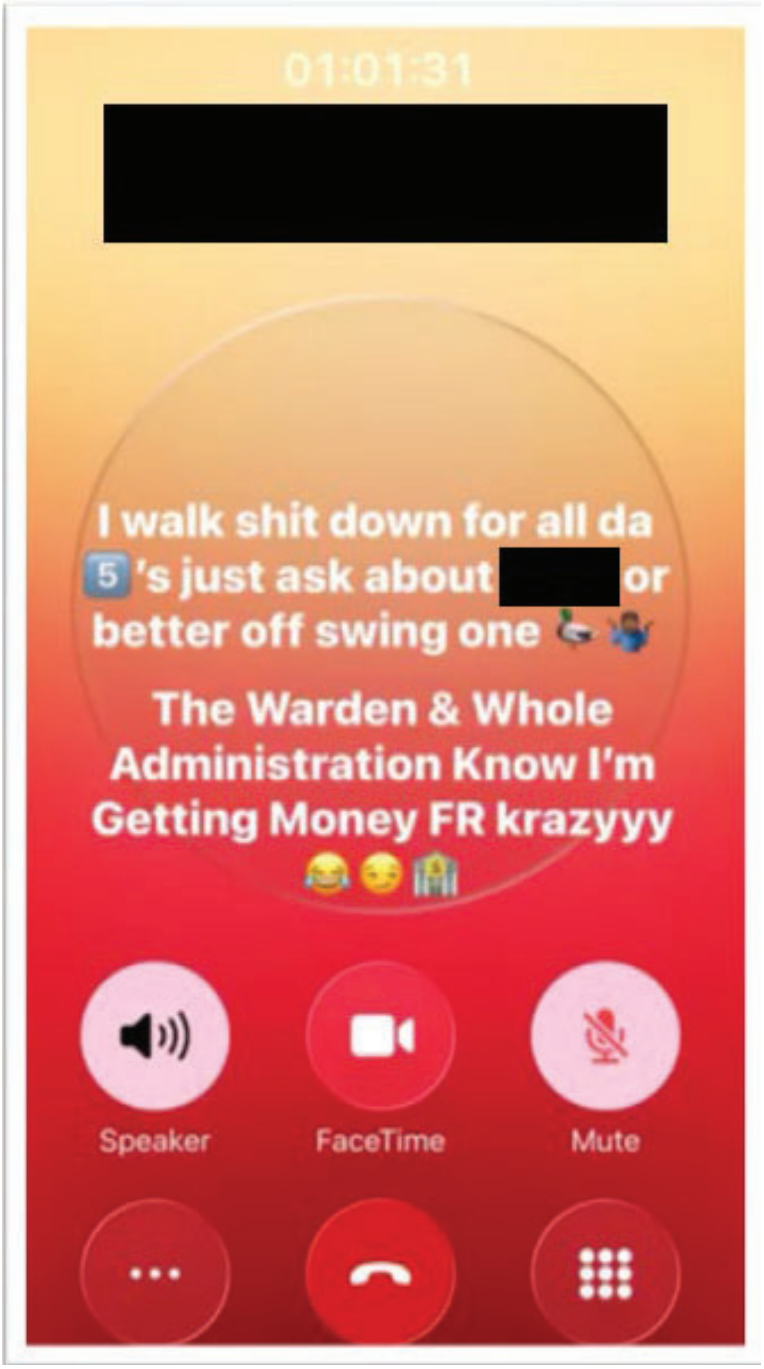


Figure 17—a Georgia inmate's Facebook post showing a phone call screenshot with a comment. The screenshot shows a one-hour telephone call in progress. Based on my review of evidence in multiple jury duty fraud investigations I believe that inmates frequently refer to victims that fall for the jury duty scam as "ducks." The reference to "walk…down" seems to be a reference to the process by which a scammer will convince and dupe a victim to paying money in the scam. Notably, the inmate's post notes that "The Warden & Whole Administration Know I'm Getting Money…" which I believe is

an acknowledgement that prison officials are at the very least aware of the criminal activities occurring in the prison and fail to disrupt it.

THE TARGET WEB HOSTING ACCOUNTS

Target Account	Domain name	Web Hosting Provider	Creation Date
1	ejurorcourts.org	InterServer, Inc.	11/22/2025
2	judicialservices.org	InterServer, Inc.	8/15/2026
3	civilservicesdivision.org	InterServer, Inc.	03/16/2026

35. Publicly available DNS records show that all three of the **TARGET WEB HOSTING ACCOUNTS** are with InterServer, Inc., located at 110 Meadowlands Parkway, Suite 100, Secaucus, NJ 07094. In other words, the data files delivered to victims and other Internet users when they visit the associated websites, the physical web servers on which those files are stored, and all account information about, or stored by, the account owner(s) are under the control of InterServer, Inc.

36. On November 2, 2026, a representative from the Administrative Office of the United States Courts confirmed to a government investigator that the **TARGET WEB HOSTING ACCOUNTS** are not official United States Courts accounts/websites.

37. As explained further below, the domain names used by the **TARGET WEB HOSTING ACCOUNTS** contain official-sounding words in an apparent attempt to impersonate an actual government agency. Secondly, the appearance of the websites for the **TARGET WEB HOSTING ACCOUNTS** shows that they share

the same website template that closely impersonates the actual uscourts.gov website. Finally, victim complaints confirm that all three sites have been used in furtherance of jury duty fraud. As further detailed, the tactics used by the scammers—impersonating law enforcement, threats of arrest, directing victims to not hang up the phone or tell anyone about the alleged proceedings against them, and the frequent use of cryptocurrency kiosks to collect payments, among other information—closely track the typical experience of jury duty victims previously described. Additional information shows that the **TARGET WEB HOSTING ACCOUNTS** appear to have been created by one entity.

WALKTHADUCK.COM

38. Based on my training and experience, I know that when a user visits a website such as those associated with the **TARGET WEB HOSTING ACCOUNTS**, the user's browser sends HTTP requests to the server hosting the site. HTTP requests ask the server hosting the website for files that make up the webpage. The website's server replies with responses containing that content, such as HTML, text, images, and fonts. Accessing a single page typically involves many HTTP requests. Some of these requests can go to third-party servers, which may be operated by the same or different companies hosting the site the user is visiting. The browser then combines all of the data it receives from these requests and renders a webpage that the user can easily view. By analyzing these HTTP requests, investigators can, among other things, identify the domains with which a browser is communicating when accessing a given site. A review of the HTTP requests for the **TARGET WEB**

HOSTING ACCOUNTS' websites shows that all three sites load or attempt to load content from another site, "walkthaduck.com." Further, walkthaduck.com and the **TARGET WEB HOSTING ACCOUNTS'** websites all resolve to the same IP address, which is associated with a subdomain of **TARGET WEB HOSTING ACCOUNT 3**, mail.civilservicesdivision.org. Given the shared IP address and HTTP requests to walkthaduck.com for each of the **TARGET WEB HOSTING ACCOUNTS**, I believe that the individuals or entities controlling walkthaduck.com are associated with the **TARGET WEB HOSTING ACCOUNTS**. A review of walkthaduck.com further confirms this association.

39. According to the website, walkthaduck.com pertains to SupaMane Technologies LLC a Georgia company registered with a registered agent service located in Atlanta.[7] The information on walkthaduck.com shows that its operators appear to be integral players in jury duty fraud schemes, by designing and hosting websites used in furtherance of the scams. First, the domain name address appears to be a reference to "walk[ing] duck[s]." As previously described in figure 18, walking ducks is a reference to the process where victims, the ducks, are duped into making payments under the false pretense that they owe fees for missing jury duty. Walkthaduck.com's "about" page claims its mission is an "awareness campaign

[7] According to Georgia Department of State records, Supamane Technologies LLC filed articles of organization on December 1, 2023 and was dissolved on or about June 14, 2024. Another company, Walk Tha Duck LLC, appears to be related and has the same registered agent and corporate address. Its articles of organization were filed on August 19, 2025 and an annual registration was filed on January 9, 2026, indicating that it was an active business as of that date.

masquerading as an official civic operation," and specifically references the use of domain names, including: "civiljuryservices.org," and "personas" such as "lieutenant" to "flip perceived authority on its head." It then states that "people think they're being summoned by 'The Man,'" which based on my training and belief appears to be a reference to false claims made by jury duty scammers to victims about missing a jury summons.

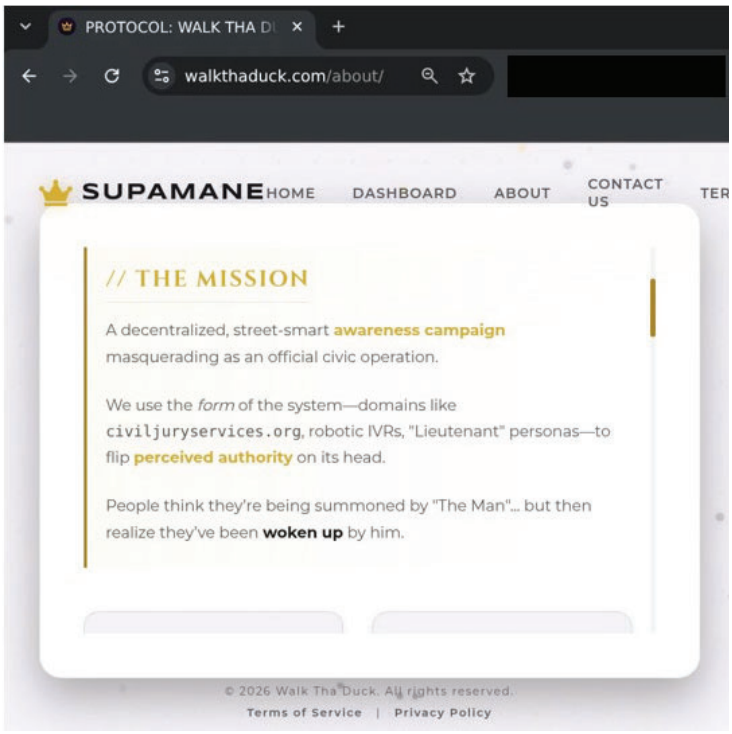


Figure 18 – screenshot of "walkthaduck.com/about," taken Oct. 26, 2026.

Further the site's terms of service displays a manifesto describing many facets of the jury duty scam:

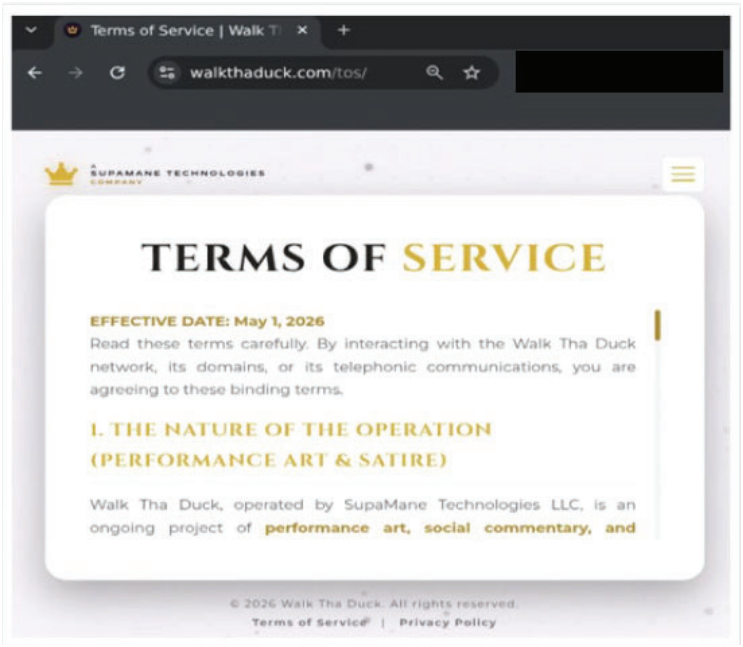


Figure 19 – screenshot of "walkthaduck.com/tos," taken Oct. 26, 2026.

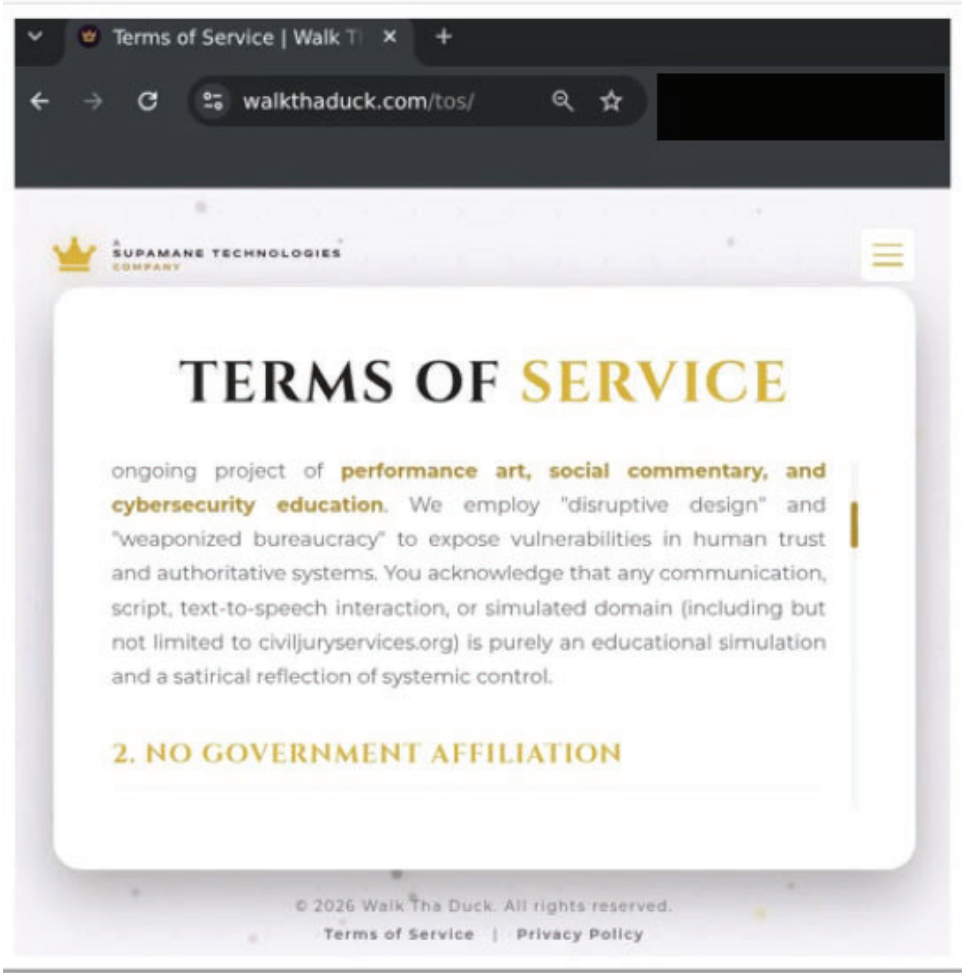


Figure 20 – screenshot of "walkthaduck.com/tos," taken Oct. 26, 2026

As seen above, the site creators again reference the website, civiljuryservices[.]org. The sites commentary claims that the owner's creation of websites is simply, art, "social commentary, and cybersecurity education." The text continues emphasizing that it has no government affiliation.

> "We are not the government. We are not the cops. Supamane Technologies LLC and Walk Tha Duck have absolutely zero affiliation with any…governmental agency, judicial system or law enforcement body. Any appearance of authority, use of terms like 'Lieutenant,' 'Court Date,' … is strictly utilized as a mirror to dissect scam mechanics and authorities' manipulation."

The disclaimers continue noting that "We do not operate as scammers. We do not extract, store, or sell your personal identifiable information (PII) for malicious intent or financial fraud." The site creators further absolve themselves of any liability for the use of "Walk Tha Duck's assets, scripts, or domains."

40. As of October 27, 2026, the website civiljuryservices.org is inactive. However, a July 30, 2025, cached image of the site shows a striking resemblance to the actual uscourts.gov website, and uses the official logo of the United States Courts. It also includes the banner stating that the site is an "official website of the United States government," and prompts the visitor to login to their account.

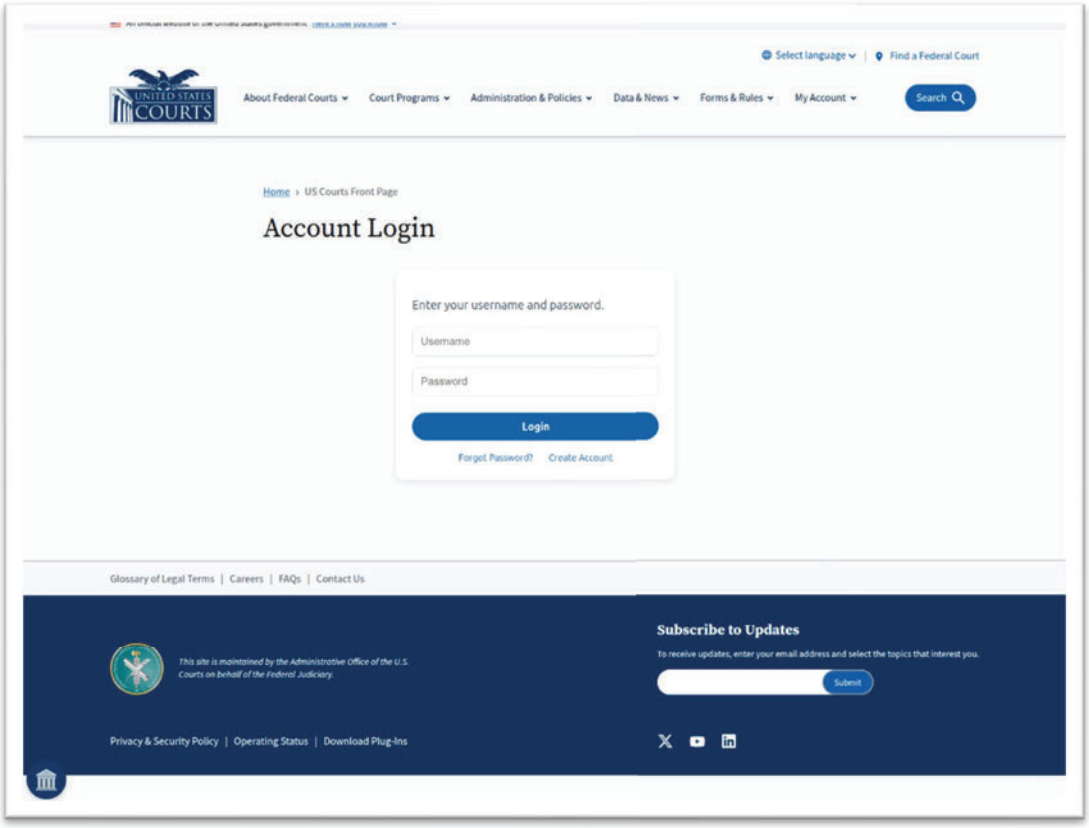


Figure 21— an image of "civiljuryservices.org," *taken July 30, 2025.*

41. Despite the creators' claims that their websites are purely a form of "performance art" and "social commentary," the webpages associated with walkthaduck.com, including civiljuryservices.org,[8] which the site explicitly takes credit for, have been the subject of over one hundred victim complaints. Victims reported to government complaint databases that they made payments in response to threats from jury duty scammers after visiting the sites associated with Walkthaduck.com.[9] Further as detailed below, victim-6, who appears to have visited the website for **TARGET WEB HOSTING ACCOUNT 3**, civilservicesdivision.org, and received emails from mail.civilservicesdivision.org, made a card payment through a subpage of walkthaduck.com, to a financial account that she labeled as "walkthaduck."

42. For example, a Texas victim reported on August 4, 2025, that he was contacted by individuals claiming to be law enforcement, who informed him that he missed jury duty. The victim was directed at Walkthaduck.com's associated website: civiljuryservices.org, to view the alleged charges filed against him. The victim stated that the website showed multiple charges and notified him that a warrant was issued for his arrest. The callers then instructed the victim to make a payment to resolve the charges. The victim reported that he made a payment of approximately $2,900.

---

[8] Similar to the other sites, HTTP requests for civiljuryservices.org similarly shows that it loads or attempts to load content from walkthaduck.com.

[9] As of October 26, 2026, civiljuryservices.org as well as the other sites referenced are inactive. The **TARGET WEB HOSTING ACCOUNTS** and walkthaduck.com are still active as of October 26, 2026.

43. On July 9, 2025, a Nebraska victim reported that she received a call from an individual claiming affiliation with her local county's sheriff's office. The caller stated that the victim had failed to appear for jury duty and would need to pay a bond fee to avoid arrest and detainment. The victim stated that she remained on the phone with the scammers, per their instructions, for the entire day, and was subject to a "gag order" which prevented her from disclosing the existence of the proceedings against her to anyone, including the bank tellers she spoke with when attempting to withdraw cash. The victim reported that she withdrew $12,500, and following the callers' instructions, deposited the cash into a crypto ATM. She further reported that during her victimization she accessed the website, uscourtsjuror.org, which according to HTTP request records, loads or attempts to load content from walkthaduck.com.

44. On January 4, 2025, a New Mexico victim reported that she spoke to an alleged lieutenant from a sheriff's department's civil services division.[10] The caller claimed that the victim failed to appear for jury duty, and that she could be detained for 72 hours. The victim visited a website, usjusticecourts.org, where she could reschedule her alleged jury duty appearance. HTTP request information shows that usjusticecourts.org is another domain that loads or attempts to load content from

[10] As explained further below, the domain name for **TARGET WEB HOSTING ACCOUNT 1** contains the same text, civil services division, and all three **TARGET WEB HOSTING ACCOUNTS'** websites feature chat windows bearing "civil services division" within the window's header. I believe that this is further confirmation that these domains are all related to Walk Tha Duck.

walkthaduck.com. The victim stated that she withdrew cash from her bank account and, following the scammers' instructions, paid approximately $12,400 using a crypto ATM.

THE DOMAIN NAMES USED BY THE TARGET WEB HOSTING ACCOUNTS

45. The domain names used by the **TARGET WEB HOSTING ACCOUNTS** contain official sounding words that I believe the scammers use to convince victims they are accessing a legitimate government website such as the US Courts official website: uscourts.gov. First, these domain names use the top-level domain (TLD): ".org"; not the official TLD for U.S. government domains: ".gov," as featured in the official US Courts website at uscourts.gov. Further the words used in the domain names indicate an attempt by the scammers to dupe victims to believe they are visiting an official government site. For example, the domain name used by **TARGET WEB HOSTING ACCOUNT 1**, ejurorcourts.org**,** begins with "ejuror," an apparent reference to the online platform ("ejuror") the US Courts use to allow citizens to complete juror qualifications questionnaires, and submit and obtain other information about their jury duty obligations. This same domain name also features the word "courts," which I believe to be an attempt to convince victims that the site pertains to an actual court. The word "judicial" in the domain name used by **TARGET WEB HOSTING ACCOUNT 2**, judicialservices.org, appears to suggest that the site has a relationship to the judicial branch of the United States government or an official legal proceeding. The word "civil" within domain name used by

TARGET WEB HOSTING ACCOUNT 3, civilservicesdivision.org, confers to victims that there is a "civil" proceeding occurring or another official process. The word "division" within this same domain name appears to be an attempt to present the site as an official "division" of the government.

SITE APPEARANCE MIMICS US COURTS

46. As displayed below, the websites for the **TARGET WEB HOSTING ACCOUNTS** are virtually identical in appearance to one another, and appear to mimic the official uscourts.gov website:

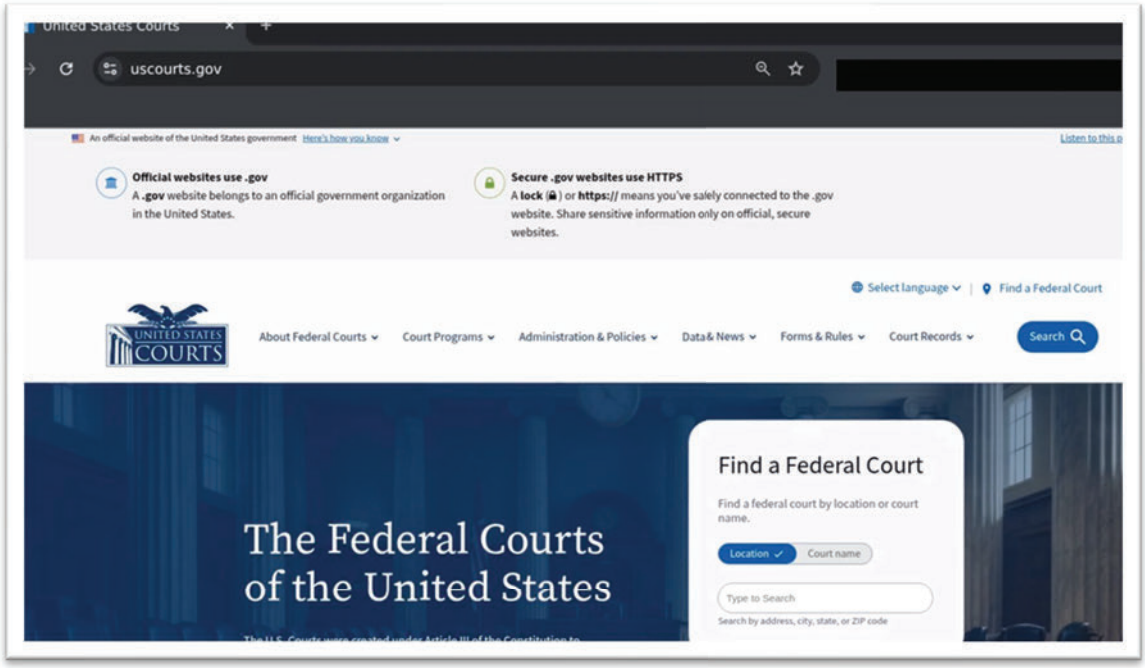


Figure 22 – the official US Courts website: uscourts.gov (accessed Oct. 23, 2026)

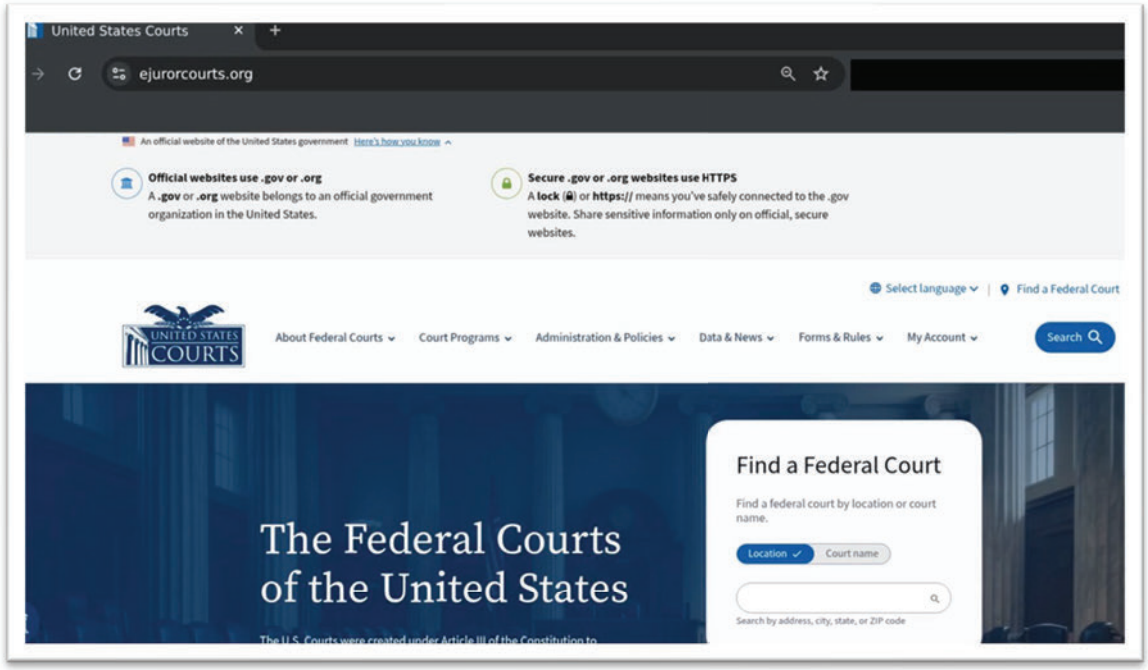


*Figure 23 – Website for **TARGET WEB HOSTING ACCOUNT 1**, ejurorcourts.org, (accessed Oct. 23, 2026)*

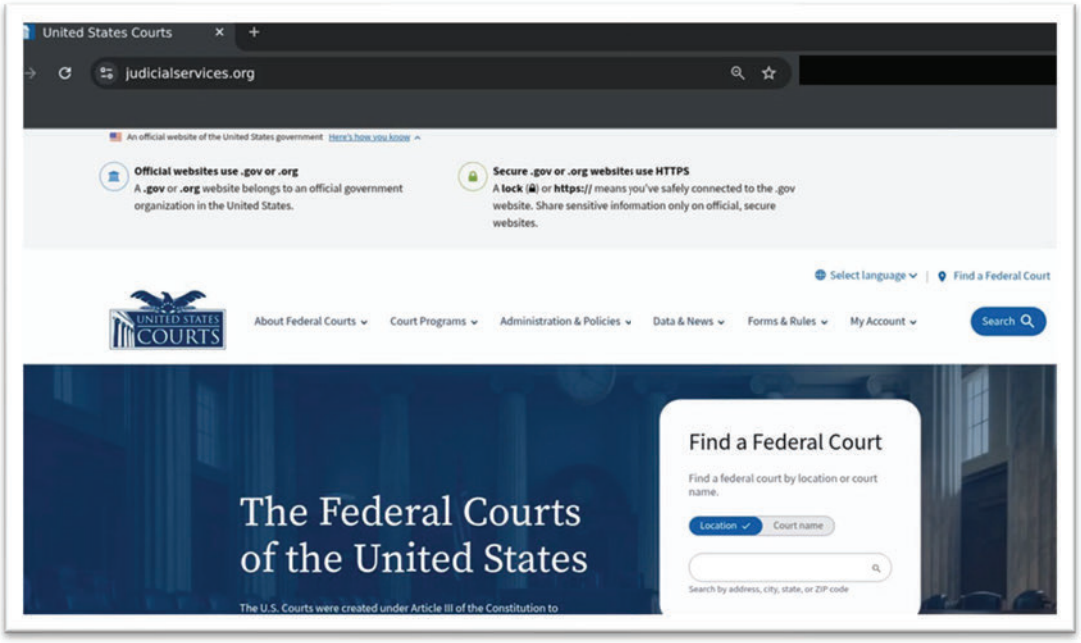


Figure 24 –Website for ***TARGET WEB HOSTING ACCOUNT 2,*** *judicialservices.org, (accessed Oct. 23, 2026)*

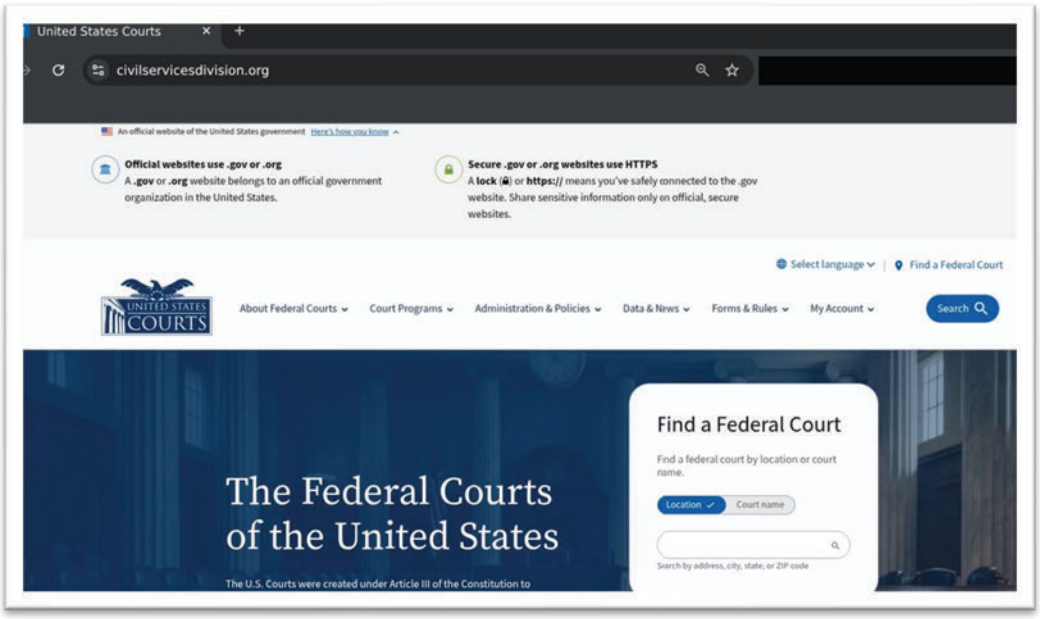


Figure 25 –Website for ***TARGET WEB HOSTING ACCOUNT 3,*** *civilservicesdivision.org, (accessed Oct. 23, 2026)*

Multiple items on the websites for the **TARGET WEB HOSTING ACCOUNTS** further indicate that the scammers are attempting to impersonate the U.S. Courts official website. First, the text, style, font, layout and logos present on these websites are virtually identical to those that appear on the official uscourts.gov site. The top grey banner on all three websites is also an imitation of the banner used for U.S. government websites. This banner is included on official U.S. government sites to confirm to the public that they are visiting an actual U.S. government website featuring the TLD ".gov," and that their connection to the site is via HTTPS, the secure protocol used to send data between a visitor's browser and the website they are accessing. As seen above, the websites for the **TARGET WEB HOSTING ACCOUNTS** contain this banner, which is almost identical to the official banner, except the scammers have altered the official site's text regarding the use of the official ".gov" domain, and the use of HTTPS. The official wording is: "A **.gov** website belongs to an official government organization in the United States." The altered wording on the websites' banner is "A **.gov or .org** website belongs to an official government organization in the United States." Similarly, the scammers have added ".org" to the banner's message regarding HTTPS: "**Secure .gov or .org websites use HTTPS**," compared to the official wording: "**Secure .gov websites use HTTPS."** Based on my review I believe the scammers added org" to this banner to convince victims that notice that they are accessing a site with .org rather than .gov, that both TLDs are official U.S. government domains, when in reality only the ".gov" domain is the official TLD for U.S. government websites.

47. The ribbon appearing below this grey banner for the websites for the **TARGET WEB HOSTING ACCOUNTS** is very similar to the ribbon on the official uscourts.gov site. This white ribbon features five options identical to the ribbon options on the official uscourts.gov site. They read from left to right: "About Federal Courts, Court Programs, Administration & Policies, Data & News, Forms and & Rules." However, the right-most option on the official site is: "Court Records" while the websites for the **TARGET WEB HOSTING ACCOUNTS** right-most option is "My Account." On the official uscourts.gov website, if a visitor clicks one of these options the site then shows a drop-down list with additional selections linking to subpages on the site. However; as of October 23, 2026, if a visitor to any of the websites for the **TARGET DOMAIN NAMES** clicks one of these options, no drop-down list appears, suggesting that the options are only included to imitate the appearance of the official site.

48. Unlike the official website, the websites for the **TARGET WEB HOSTING ACCOUNTS** include a blue circle with a court icon appearing at the bottom left of the user's browser when they access the page. When clicked, the icon opens a chat window, as displayed below:

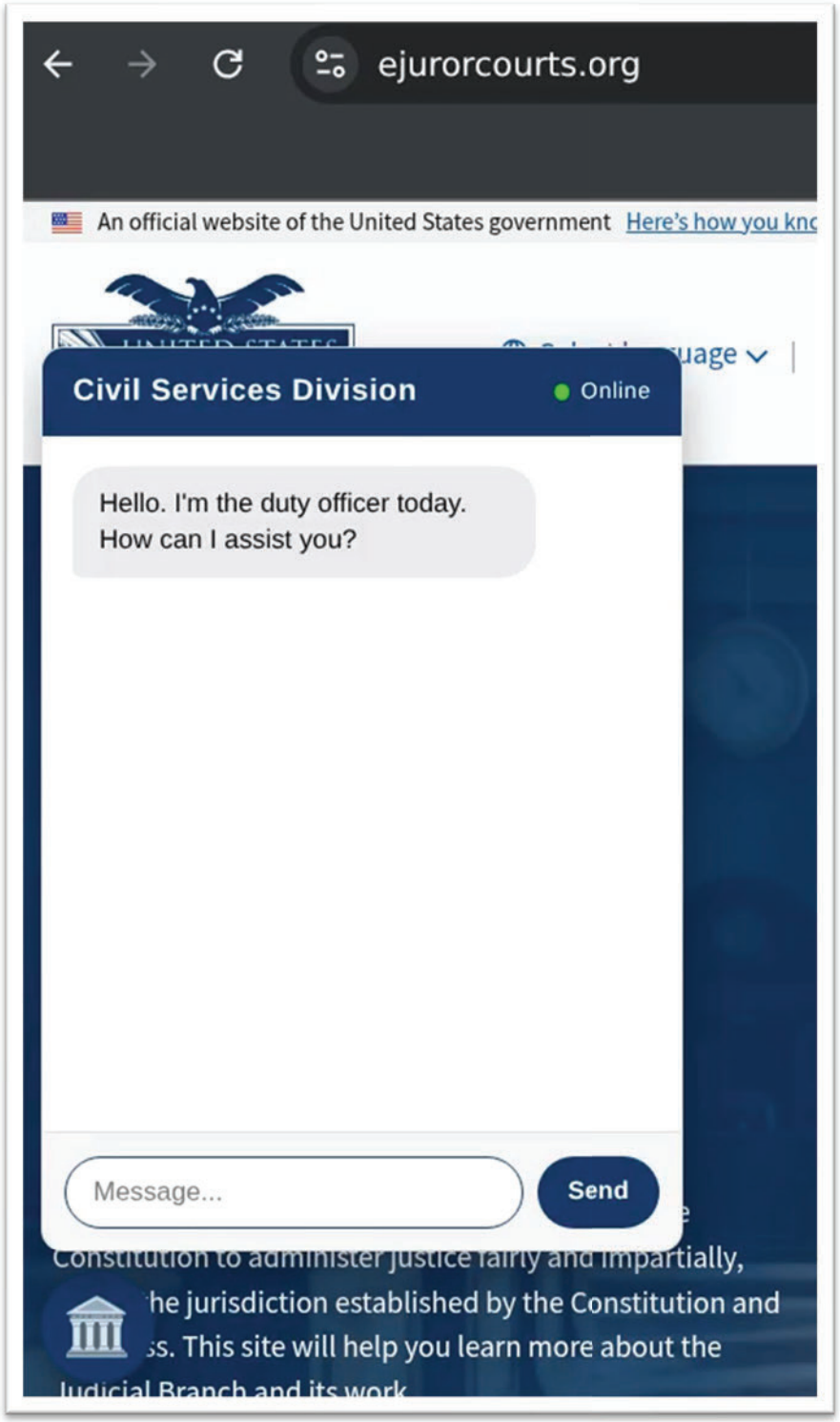


Figure 26—screenshot of ***TARGET WEB HOSTING ACCOUNT 1*** *website's chat window (accessed Oct. 23, 2026).*

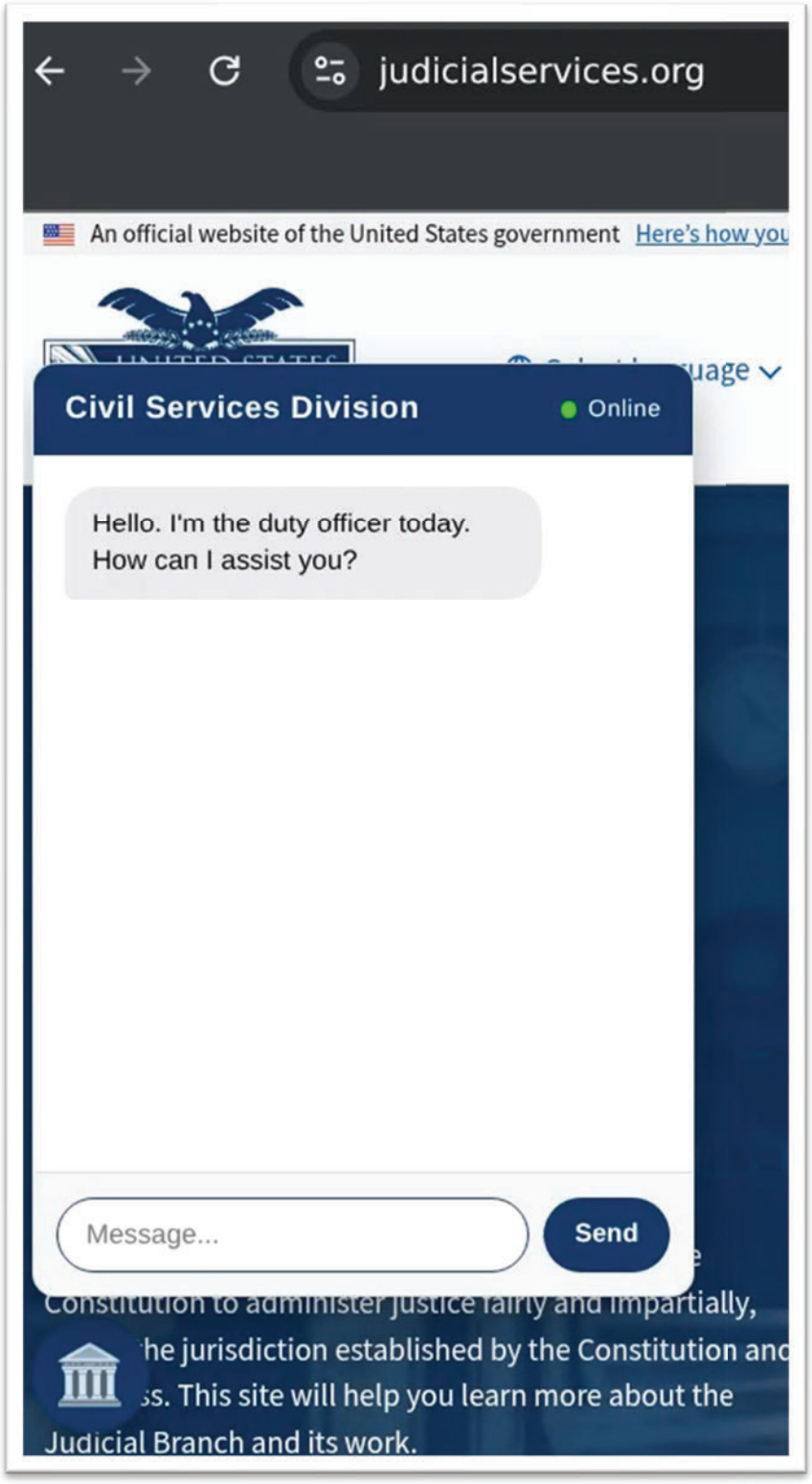


Figure 27—screenshot of ***TARGET WEB HOSTING ACCOUNT 2*** *website's chat window (accessed Oct. 23, 2026)*

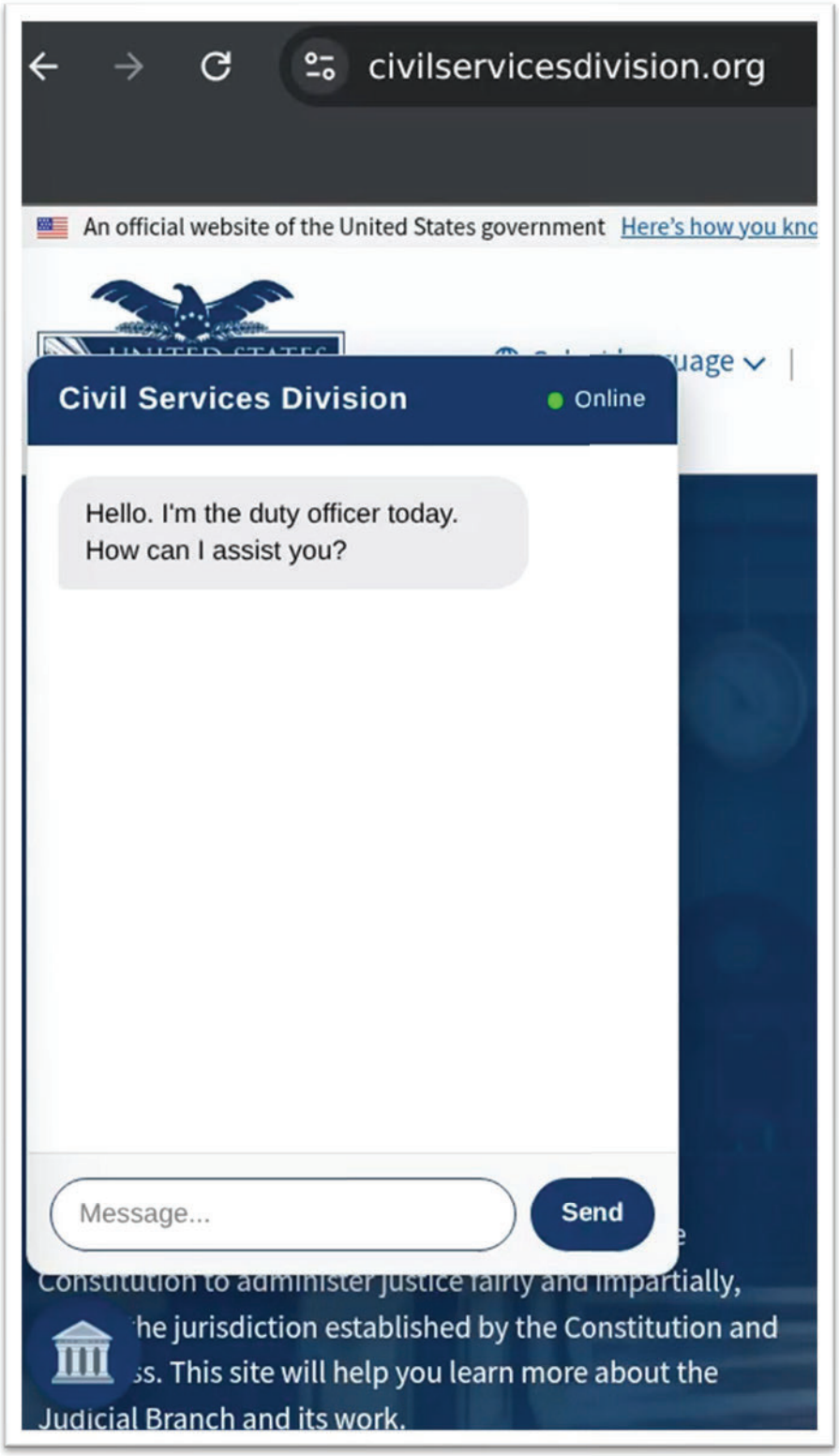

civilservicesdivision.org
An official website of the United States government
Here's how you kno
Civil Services Division
Online
Hello. I'm the duty officer today.
How can I assist you?
Message...
Send
Constitution to administer justice fairly and impartially,
he jurisdiction established by the Constitution and
ss. This site will help you learn more about the
Judicial Branch and its work.

*Figure 28—screenshot of **TARGET WEB HOSTING ACCOUNT 3** website's chat window (accessed Oct. 23, 2026)*

All three chat windows, feature a header indicating that they pertain to the "Civil Services Division" which is a name reminiscent of the domain **TARGET WEB HOSTING ACCOUNT 3**. I believe that the use of this header, "Civil Services Division," is further evidence that the three sites were created by the same individuals or entities. The question appearing in the chat: "Hi I'm the duty officer today. How can I assist you?" appears to be an attempt by scammers to pose as law enforcement, the "duty officers," when communicating with victims. As previously described, jury duty victims report communicating with law enforcement officers during their victimization.

VICTIM COMPLAINTS

TARGET WEB HOSTING ACCOUNT 1: ejurorcourts.org

49. Victim complaints regarding the **TARGET WEB HOSTING ACCOUNTS** further show that all three websites are used in furtherance of jury duty schemes. Regarding **TARGET WEB HOSTING ACCOUNT 1**, Maryland victim-1 reported on a government complaint website that on February 9, 2026, she spoke with a caller claiming to be lieutenant with her local county's sheriff's department. Victim-1 stated that she received calls from phone numbers that matched her county's publicly available non-emergency number. The caller informed victim-1 that she failed to appear for jury duty, and a judge had issued a warrant for her arrest. The caller further stated that if victim-1 entered government property

while the warrant was "active," she would be jailed for "3045 days." The caller instructed victim-1 to make a bail payment that would later be refunded to her and not to inform anyone about the existence of the proceedings against her. Victim-1 stated that the caller emailed her a link to the website for **TARGET WEB HOSTING ACCOUNT 1,** ejurorcourts.org. Victim-1 was informed that she needed to access the site to verify her information. She stated that she accessed that website and input her social security number, date of birth, and home address. She stated that, after she provided this information, the site displayed a document listing charges and fines levied against victim-1 and said that she needed to make a bail payment of $12,350. The caller instructed victim-1 to drive to a "bonding kiosk" to pay this fee. Victim-1 stated that, at this point, she became suspicious of the callers' claims and after searching online, discovered that the callers were attempting a jury duty scam.

50. On January 6, 2026, victim-2, an elderly woman located in Texas reported that she was contacted by individuals claiming to be from a county Sheriff's office. The callers, including one who identified himself as a lieutenant, stated that there was a federal warrant for her arrest because she failed to appear for jury duty. The callers stated that there was an alleged "gag order" against her, and that, in order to avoid arrest and 30 days in jail, she needed to pay $10,000 using a "kiosk machine." Victim-2 traveled to her bank and withdrew cash from her bank account. She noted that the bank teller asked her about the purpose of the withdrawal, and that the caller, with whom she was still talking on the phone, instructed victim-2 to claim that the cash withdrawal was for "repairs." After she withdrew the cash,

victim-2 expressed doubts to the callers about the process. They then instructed her to access an alleged official website at **TARGET WEB HOSTING ACCOUNT 1,** ejurorcourts.org, where she input her personal information. The site then provided her with information regarding the alleged warrant filed against her, and the fees she owed. The scammers directed victim-2 to drive to a crypto ATM where she deposited $10,000 to pay the alleged fees for missing jury duty. When the scammers claimed that victim-2 needed to make an additional payment, she refused, ended the call, and reported the scam in person to her local sheriff's office. Victim-2 stated that she was on the phone for over 6 hours.

TARGET WEB HOSTING ACCOUNT 2: judicialservices.org

51. On September 6, 2026, victim-3, located in Colorado, reported that she received a phone call from an individual who claimed she was subject to an investigation for failing to appear for jury duty. The caller directed victim-3 to visit the website for **TARGET WEB HOSTING ACCOUNT 2**, judicialservices.org. Victim-3 noted that she saw the banner at the top of the webpage claiming that it was a real United States government site because the domain name address ended in ".org." The caller provided instructions to victim-3 to input personal information into the site. After victim-3 repeatedly questioned the caller regarding the legitimacy of his claims, the caller claimed that he would transfer her to the "criminal division" and then ended the call.

52. On August 31, 2026, victim-4, located in Washington, reported that she received a call from individuals who claimed she missed jury duty and that there was

a warrant for her arrest. The callers informed victim-4 that she needed to make a $7,000 bail payment, which would immediately be refunded. The callers also threatened to detain victim-4 for 5-10 months if she spoke with anyone about the proceedings against her. She was then directed to visit the website for **TARGET WEB HOSTING ACCOUNT 2**, judicialservices.org, which she described as identical to the US courts webpage, and created an account by inputting her social security number and other personal information.

53. On September 11, 2026, victim-5, located in Nevada, reported that he received a phone call while at work from an alleged officer from a sheriff's department. The caller informed him that there was a warrant issued for his arrest for failing to appear for jury duty. The caller directed victim-5 to drive to a local police department and to remain on the phone line the entire time. During the drive, the callers directed victim-5 to pull over. The callers emailed victim-5 an alleged jury summons. The callers informed victim-5 that he needed to obtain a bail receipt by making a payment prior to arriving at the police department. The email sent to victim-5, from an address in the domain name associated with **TARGET WEB HOSTING ACCOUNT 2**, alleged that victim-5 "failed to appear for federal grand jury duty as required by law," and that "failure to respond may result in additional fines, a bench warrant or other legal actions." The email also stated that "fines for non-attendance can be paid through our online payment center or in person at a federal bonding kiosk." The email instructed victim-5 to "complete your juror registration to reschedule . . ." and included a link to the website for **TARGET WEB**

HOSTING ACCOUNT 2, judicialservices.org. Victim-5 reported that he drove to a business with a crypto ATM, deposited over $12,000, and completed a payment scanning a QR code linking to a crypto address provided by the scammers. After completing the transaction, victim-5 grew suspicious when the machine did not provide a receipt of his payment, which the scammers said he needed to have prior to arriving at the police station. Victim-5 stated that the scammers later requested additional money which further increased his skepticism. When victim-5 arrived at the actual sheriff's office, the caller disconnected.

TARGET WEB HOSTING ACCOUNT 3: civilservicesdivision.org

54. Victim-6, located in New York, reported that on May 1, 2026, she received a threatening call from individuals claiming to be officers with the U.S. government. These callers claimed that she needed to make payments for missing jury duty and avoid arrest. Victim-6 stated that the callers provided her with a website, which I believe to be that for **TARGET WEB HOSTING ACCOUNT 3**,[11] that appeared to be a webpage pertaining to a "legitimate court." She stated that the callers directed her to pay using a peer-to-peer platform as well as a credit card. Victim-6 noted that she completed the credit card payments through the site "https://pay.walkthaduck.com/c/pay/cs," a subpage of "walkthaduck.com." She

[11] Victim-8 did not specifically list the website for **TARGET WEB HOSTING ACCOUNT 3,** civilservicesdivision.org, as the site she visited within the complaint. However, she indicated that she received emails from info@civilservicesdivision.org and, as indicated in her complaint, her description of the site matches the content on the website for **TARGET WEB HOSTING ACCOUNT 3**.

further indicated the recipient account name for these payments was "Walkthaduck." She further indicated that she was extremely scared by the call and it occurred during a time when she felt particularly vulnerable because she was away from her home dealing with the death of a family member. As previously stated, I believe that this payment provides further evidence that walkthaduck.com and its owners are integrally involved in jury duty fraud, because their website facilitated victim payments to financial accounts in the name of "walkthaduck."

55. On May 16, 2026, victim-7, in the Eastern District of Virginia, stated that she received and returned a call from an alleged sheriff who informed her that she missed jury duty and could be arrested. The caller instructed her to remain on the phone line and deposit $3,500 into a crypto ATM to pay an alleged bond and avoid arrest. The caller also directed her to navigate to the website for **TARGET WEB HOSTING ACCOUNT 3**, civilservicesdivision.org, and provide personal information, including an image of her driver's license and social security number to "start the process." Victim-7 stated that she drove to a gas station with a crypto kiosk to make the payment, but a sign above the kiosk alerted her to their use in scams. Victim-7 grew suspicious and decided not to send money to the scammer.

TARGET WEB HOSTING ACCOUNTS' INVOLVEMENT IN MONEY LAUNDERING

56. Based on all the facts detailed above, I believe that the **TARGET WEB HOSTING ACCOUNTS** and associated websites are used by scammers to convince victims that they are communicating with actual law enforcement; that they missed

jury duty; and, that they need to make payments to avoid legal consequences. Thus, there is probable cause to believe that they are key facilitating property of money laundering conspiracies. Scammers induce U.S. victims to send payments, including payments to cryptocurrency addresses controlled by the jury duty scammers and payments directly to an entity, "walkthaduck," registered in the Northern District of Georgia. As described, there is probable cause to believe that this entity, through its website walkthaduck.com, is directly related to the **TARGET WEB HOSTING ACCOUNTS**. These actions promote money laundering conspiracy schemes. In other words, these scam domains facilitate the transfer of funds derived from a specified unlawful activity (conspiracy to commit wire fraud, in violation of 18 U.S.C. § 1349) from locations throughout the United States to the Northern District of Georgia to promote the carrying on of that specified unlawful activity, in violation of 18 U.S.C. §§ 1956(a)(1) and (h).

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

57. Title 18, United States Code, Section 981(a)(1)(A) provides, in relevant part, that any property involved in, or traceable to property involved in a violation of Title 18, United States Code, Section 1956, is subject to civil forfeiture to the United States government.

58. Title 18, United States Code, Section 982(a)(1) provides, in relevant part, that any property involved in, or traceable to property involved in a violation of

Title 18, United States Code, Section 1956, is subject to criminal forfeiture to the United States government.

59. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause. Title 18, United States Code, Section 981(b)(3) permits the issuance of a seizure warrant by a judicial officer in any district in which a forfeiture action against the property may be filed and may be executed in any district in which the property is found.

60. Title 18, United States Code, Section 982(b)(1) authorizes the issuance of a criminal seizure warrant under Title 21, United States Code, Section 853(f), which provides in relevant part that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

61. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the **TARGET WEB HOSTING ACCOUNTS** for forfeiture. By seizing the **TARGET WEB HOSTING ACCOUNTS**, the Government will prevent third parties from using these resources to commit additional crimes.

62. As set forth above, there is probable cause to believe that the **TARGET WEB HOSTING ACCOUNTS** are subject to civil and criminal forfeiture because

they were involved in, or traceable to property involved in, a violation or violations of Title 18, United States Code, Section 1956.

SEIZURE PROCEDURE

63. Upon execution of the seizure warrant, InterServer, Inc., located at 110 Meadowlands Parkway, Suite 100, Secaucus, NJ 07094, shall be directed to restrain and lock the **TARGET WEB HOSTING ACCOUNTS** pending transfer of all right, title, and interest in the **TARGET WEB HOSTING ACCOUNTS** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET WEB HOSTING ACCOUNTS** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Postal Inspection Service or the Department of Justice.

64. In restraining and locking the accounts, Interserver shall ensure that

a. complete copies of all data stored in each of the **TARGET WEB HOSTING ACCOUNTS** – including but not limited to data files which comprise complete copies of application environments, database instances, and full virtual server machine images (including operating

system configurations and system logs) – are made and securely retained;

b. the websites belonging to each of the **TARGET WEB HOSTING ACCOUNTS** are rendered inaccessible from the Internet; and

c. the **TARGET WEB HOSTING ACCOUNTS'** customer-owners are no longer able to access their accounts or any account data or associated system resources.

CONCLUSION

65. For the foregoing reasons, I submit that there is probable cause to believe that the **TARGET WEB HOSTING ACCOUNTS** were involved in, or traceable to property involved in, a violation or violations of Title 18, United States Code, Section 1956.

66. Accordingly, the **TARGET WEB HOSTING ACCOUNTS** are subject to forfeiture to the United States pursuant to the authority recited above and I respectfully request that the Court issue a seizure warrant for the **TARGET WEB HOSTING ACCOUNTS**.

67. Finally, and in order to protect the ongoing investigation and in consideration that much of the information set forth above is not otherwise publicly available, I respectfully request that this Affidavit be filed and kept under seal until further order of this Court.

68. Because the warrant will be served on InterServer, Inc., which controls the **TARGET WEB HOSTING ACCOUNTS**, and InterServer, Inc.**,** thereafter, at a time convenient to it, will transfer control of the **TARGET WEB HOSTING**

ACCOUNTS to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night

Respectfully submitted,

/s/ [redacted] */SN*

[redacted]
Inspector
United States Postal Inspection Service

Subscribed to and sworn before me on this 5th day of November, 2026.

/s/ Jessica S. Allen/SN

Hon. Jessica S. Allen
United States Magistrate Judge

ATTACHMENT A

With respect to judicialservices.org, ejurorcourts.org, and civilservicesdivision.org (the "**TARGET WEB HOSTING ACCOUNTS"**), InterServer, Inc., located at 110 Meadowlands Parkway, Suite 100, Secaucus, NJ 07094, shall restrain and lock the **TARGET WEB HOSTING ACCOUNTS** pending transfer of all right, title, and interest in the **TARGET WEB HOSTING ACCOUNTS** to the United States upon completion of forfeiture proceedings, to ensure that changes to the **TARGET WEB HOSTING ACCOUNTS** cannot be made absent court order or, if forfeited to the United States, without prior consultation with United States Postal Inspection Service or the Department of Justice.

1. In restraining and locking the accounts, Interserver shall ensure that

   a. complete copies of all data stored in each of the **TARGET WEB HOSTING ACCOUNTS** – including but not limited to data files which comprise complete copies of application environments, database instances, and full virtual server machine images (including operating

system configurations and system logs) – are made and securely retained;

b. the websites belonging to each of the **TARGET WEB HOSTING ACCOUNTS** are rendered inaccessible from the Internet; and

c. the **TARGET WEB HOSTING ACCOUNTS'** customer-owners are no longer able to access their accounts or any account data or associated system resources.

The Government will display a notice on the website to which the **TARGET WEB HOSTING ACCOUNTS** will resolve. That notice will consist of law enforcement emblems and text (or substantially similar text) as shown on the attached page.

