AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

FILED
MAR 20 2019
U.S. DISTRICT COURT
EASTERN DISTRICT OF MO
ST. LOUIS

for the

Eastern District of Missouri

In the Matter of the Search of

Steven Stenger and a cellular device using cellular phone number [redacted]

Case No. 4:19 MJ 7099 SPM

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the EASTERN District of MISSOURI *(identify the person or describe the property to be searched and give its location)*:

Steven Stenger and a cellular device using cellular phone number [redacted]

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

YOU ARE COMMANDED to execute this warrant on or before April 3, 2019 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to United States Magistrate Judge Shirley P. Mensah.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: 3.20.2019. 17:02

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

Return		
Case No.: 4:19 MJ 7099 SPM	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

The person to be searched is Steven Stenger (the "SUBJECT PERSON"), who resides at 336 N. Forsyth Blvd., St. Louis, Missouri. The SUBJECT PERSON is a 47 year-old white male, standing approximately 5 feet 10 inches tall, and weighing approximately 200 pounds. The SUBJECT PERSON is depicted in the photograph below:

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, in any format or medium, which constitute evidence, instrumentalities, and fruits of the criminal violations of 18 U.S.C. § 666, § 1343, and §1951 and involve Steven Stenger, and others from October 23, 2014, through the time of the execution of this warrant that may be deemed instrumentalities, fruits, or evidence of the aforementioned crimes to include:

1. The cellular phone, that being an Apple iPhone X, serial number G6TWRPFBJCL7 with associated phone number [redacted]. (The Device)

2. For the Device, all records and information to include:

a. Call Logs showing numbers called and received, to include deleted logs;

b. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

c. Internet browsing history, including records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search ter1USAOms that the user entered into any Internet search engine, and records of user-typed web addresses.

d. Photographs, videos, and other forms of media documenting the events that are the subject of this warrant.

e. Any and all contact lists, address books, in whatever form regarding coconspirator

contact information, to include deleted information.

f. all bank records, checks, credit card bills, account information, and other financial records.

g. Text message records, including the content of messages as well as any logs showing text messages sent and received, to include deleted information

h. Any and all documents, notes, and records, including e-mail correspondence in whatever form, including digital, relating to the matters set forth in the attached Affidavit, to include deleted information

i. Any and all documents, notes, and records relating to the ownership and usage of the cell phone being searched

j. Any and all contact lists, address books, in whatever form regarding coconspirator contact information, to include deleted information

3. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingers and/or thumbprints of Steven Stenger onto the Touch ID sensor of any Apple iPhone with Touch ID, and or initiate facial recognition a/k/a Apple Face ID feature belonging to this individual for the purpose of attempting to unlock the device via Touch ID or facial recognition in order to search the contents of the phone as authorized by this warrant

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of Missouri

In the Matter of the Search of

Steven Stenger and a cellular device using cellular phone number [redacted]

Case No. 4:19 MJ 7099 SPM

APPLICATION FOR A SEARCH WARRANT

I, Andrew R. Ryder, 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 property:

~Steven Stenger and a cellular device using cellular phone number [redacted]

located in the EASTERN District of MISSOURI, there is now concealed

SEE ATTACHMENT B

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*
18 U.S.C. Section 666(a)(1)(A)	Theft or bribery concerning programs receiving Federal funds
18 U.S.C. Section 1346	Honest Services Fraud
18 U.S.C. Sections 1341 and 1343	Mail and Wire Fraud
18 U.S.C. Section 1951	Hobbs Act

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE

- ☑ 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.

Applicant's signature

Andrew R. Ryder
Special Agent, Federal Bureau of Investigation
Printed name and title

Sworn to before me and signed in my presence.

Date: 3.20.2019

Judge's signature

City and state: St. Louis, MO

Honorable Shirley Padmore Mensah, U.S. Magistrate Judge
Printed name and title

AUSA: Hal Goldsmith

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF MISSOURI

In the Matter of the Search of **Steven Stenger** and a cellular device using cellular phone number [redacted]	Case No. 4:19 MJ 7099 SPM **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH AND SEIZURE WARRANT

I, Special Agent Andrew R. Ryder, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant to search and seize instrumentalities and evidence of violations of Title 18 U.S.C. §§ 666(a)(1)(A), 1951, 1341, 1343, 1346, and 2 belonging to Steven Stenger, the St. Louis County Executive. The item that is the subject of the search applied for in this affidavit is the person of Steven Stenger and an Apple iPhone X, serial number G6TWRPFBJCL7 with associated phone number [redacted] operated by Stenger (The Device) for the purpose of searching for evidence of violations of Title 18 U.S.C. §§ 666(a)(1)(A), 1951, 1341, 1343, 1346, and 2 related to the awarding of lucrative St. Louis County contracts and other County business to campaign donors. There is probable cause to believe that evidence of these violations will be found on the person identified in Attachment A and the cellular telephone identified in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed since 2002. I am presently assigned to the Public Corruption squad in the St.

Louis Division of the FBI. My responsibilities include the investigation of federal crimes to include violations of Title 18 United States Code (U.S.C.) § 666 (Theft or bribery concerning programs receiving Federal funds), § 1346 (Honest Services Fraud), § 1341 (Mail Fraud) and § 1343 (Wire Fraud) and §1951 (Hobbs Act). I received over eighteen weeks of specialized law enforcement training at the FBI Academy in Quantico, Virginia. My experience obtained as a Special Agent of the FBI has included investigations of multiple violations of federal criminal public corruption laws. I know cellular telephones are commonly used by politicians to communicate with donors, constituents, and employees. Cellular telephones enable a politician to communicate during the day when they are not at an office location, which is common with this type of work. Cellular telephones also enable the user to quickly send text messages to other people when they are unable to take the time to make a phone call, but the sender needs to quickly convey their message.

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. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of inter alia, 18 U.S.C. § 666 (Theft or bribery concerning programs receiving Federal funds), § 1343 (Wire Fraud), and §1951 (Hobbs Act) have been committed by Steven Stenger, St. Louis County Executive. There is also probable cause to search Steven Stenger identified in Attachment A and the Device identified in Attachment B for the information described in Attachment B for evidence of these crimes and contraband or fruits of these crimes, as described in Attachment B.

PROBABLE CAUSE

5. On March 5, 2018, the FBI opened an investigation based on an allegation the Executive Director of the St. Louis County Port Authority, Sheila Sweeney, used Port Authority funds to pay Cardinal Creative Consulting $130,000 for a 2016 consulting contract. The original allegation indicated the contract was payback for political donations made to St. Louis County Executive Steven Stenger, and little or no work was actually performed under the consulting contract. Multiple sources of information, including individuals named below, have described to myself and others at the FBI a pattern whereby St. Louis County Executive Steve Stenger directs contracts and grants to be awarded to individuals and companies who have made political contributions to Stenger. When Stenger lost the ability to utilize the St. Louis County Council to award contracts to donors because of conflicts between him and several Council Members, he recognized the opportunity to use money from the St. Louis County Port Authority for this purpose. The St. Louis County Port Authority has an annual operating budget of approximately $4.0 million. Shortly after Sweeney was appointed by Stenger as Executive Director in September 2015, Stenger began directing the actions of the Port Authority through Sweeney. In addition to the Cardinal Creative contract, multiple other contracts and grants were directed by Stenger, using Sweeney and the Port Authority, for political donors to Stenger.

6. [redacted]

a. Rallo [redacted] met St. Louis County Executive Steven Stenger in or around October 23, 2014 at Sam's Steakhouse in St. Louis County. Rallo's friend Sorkis Webbe, Jr. set up the meeting in order to introduce Rallo and Stenger. Rallo met with

Stenger with the hope of securing a benefit in exchange for a political donation. Rallo told Stenger he wanted a "fair shot" at obtaining the county's employee benefits insurance contract through his company Cardinal Insurance. Rallo gave Stenger a $5,000 political donation at that dinner, in exchange for Stenger's promise to help him get the St. Louis County insurance contract. Stenger told him he could make the contract a reality as those involved with the approval process "are under me." Rallo told Stenger that he was tired of giving money to politicians and not getting anything in return. Stenger told him, "That won't happen with me." Rallo wrote two campaign donation checks that evening totaling $5,000, and handed them to Stenger at the dinner table.

b. Despite efforts by Stenger to direct the County's employee voluntary benefits insurance contract to Rallo and Rallo's company during 2015 and 2016, for various reasons Rallo was not awarded the contract. Stenger's efforts included directing both the County Chief of Policy and the County Director of Operations to work with Rallo and "make sure" Rallo's company was awarded the insurance contract. Stenger also communicated to the County Director of Administration his preference that Rallo be awarded the insurance contract. Nonetheless, the County administration determined to stay with the incumbent insurance company, and Rallo's company never received the insurance contract as had been promised by Stenger.

c. The 2016 consulting contract was a "payback contract" for Rallo's insurance company not receiving the St. Louis County voluntary benefits insurance contract which St. Louis County Executive Steve Stenger had promised to Rallo. The

contract was promised in return for a series of political donations made by Rallo to Stenger. Rallo and a business partner he recruited contributed approximately $45,000 to Stenger up through April, 2018, and Rallo also held several fundraisers for Stenger which raised additional funds for Stenger from Rallo friends and associates. Rallo's close friend, television personality Montel Williams, was purportedly going to work with Rallo on the consulting contract, but Williams actually performed no work, and was not involved in the negotiations to obtain the contract.

d. At Stenger's direction, beginning on or about October 2015, SLCPA Executive Director Sheila Sweeney met with Rallo on multiple occasions to discuss the consulting contract amount. Stenger told Rallo that Sweeney has the money in her Port Authority budget, and she does not have to go through the County Council to get approval. Rallo proposed $350,000 to Sweeney, but it was ultimately agreed upon at $100,000 for a six month term, potentially renewable for an additional $100,000.

e. Sweeney told Rallo [redacted] helped get Stenger the North County vote during the November, 2014 election for County Executive, and Stenger needed to get money to "[redacted] guy", an individual named J[redacted] C[redacted]. Shortly after the Cardinal Creative consulting contract was awarded at $100,000, Sweeney told Rallo she was adding $30,000 to the consulting contract because Steve Stenger had "a guy he needs to take care of." Sweeney told Rallo to pay the additional $30,000 to J[redacted] C[redacted]. C[redacted] did not do any actual work on the Cardinal Creative consulting contract, but Rallo paid him $25,000 ($5,000 less than

what he had been directed to pay C[redacted]). During that time, [redacted] Sweeney saying to Rallo, "What did I get myself into" in regard to having to "take care of Stenger's people".

f. In December 2017 there were a series of negative St. Louis Post Dispatch articles about the Cardinal Creative consulting contract and Rallo's political donations to Stenger. At or about that time, Sweeney told Rallo to remove his name as Registered Agent for Cardinal Creative on the Missouri Secretary of State website. [redacted] Sweeney did not want people to be able to see Rallo was associated with companies that were awarded contracts through the Port Authority. Sweeney texted Rallo, "Got to cover him! And me too!!!!" referring to protecting Stenger and Sweeney. Rallo [redacted] found a lawyer and removed his name as Registered Agent for Cardinal Creative as Sweeney had instructed.

g. Rallo [redacted] had no consulting experience, his bid was "complete bullshit", and this contract was 100% due to political donations he had made to Stenger. There were several other companies with real marketing experience which bid on the consulting contract, at lower prices than Rallo's bid, but Rallo was awarded the contract at Stenger's direction.

h. [redacted] Sweeney was directed by Stenger to pay C[redacted] under the consulting contract. After Stenger directed Sweeney to award the

consulting contract to Rallo and Cardinal Creative, the project moved forward with "zero bumps."

i. Rallo [redacted] primarily texted with Stenger and he did not correspond with him via e-mail. [redacted] one of the phones carried by Stenger was an Apple device.

7. An FBI forensic review of Rallo's cellular phone identified a series of text messages between Rallo and Stenger [redacted]

a. On October 28, 2015, Rallo sent Stenger a text message, "Spoke w/Sheila (Sweeney) re: Montel…sounds like things are not going to move forward. Diametrically different from our conversation in your office. Let me know when you have a min to talk." Stenger, using cellular telephone [redacted], replied by text, "The 350k won't work for their budget but some other amount would. Needs to be negotiated."

b. On January 13, 2016, Stenger, using cellular telephone [redacted], sent a text to Rallo, "Have you made contact with Sheila at the partnership since we spoke?" Rallo responded, "I have not, I was going to send you a one page bullet pt outline as we discussed. Should I reach out to her again directly?" Stenger replied by text, "Shoot me the one pager when u can. I am meeting with Jeff [Jeff Wagner, County Chief of Policy] now talking about things we need to take care of soon and this was on my agenda."

c. During a text message exchange starting on March 28, 2016, Stenger asked Rallo for campaign money (Citizens for Steve Stenger) to come in before the end of the quarter, "John, is there a way we would be able to get your 2500 for the quarter dated 3.31

in the next few days so we could count it for this quarter. We are trying to hit 300k for the quarter and it would be helpful." After the two arrange for pick up of the check, on March 31, 2016 Rallo replies, "Check is ready! Need 5 min call to go over a concern I have on the insurance RFP…are u avail later today?" [redacted] the best time to ask Stenger for a contract or other benefit was immediately after Rallo gave Stenger money. There were other text messages where Rallo asked Stenger for a one-on-one or alone meeting. The purpose of these meetings was for Rallo to make it clear to Stenger he (Rallo) gave money and he wanted a deal.

8. [redacted]

a. In September 2015, Sweeney became the Executive Director of the SLCPA, having been appointed by Steve Stenger. She quickly learned that any projects that came to the Port Authority had to be run by Stenger before deciding on them. Stenger saw the Port Authority money as the perfect place to avoid the St. Louis County Council. If Sweeney did not consult with Stenger before making a decision, the "wrath" of Stenger would come down on Sweeney. [redacted] there were very few contracts or grants at the Port Authority that Stenger didn't personally direct. In many of these instances Stenger told Sweeney the contract/grant was for a political donor.

b. In a meeting in Stenger's office, Stenger told Sweeney that John Rallo was a donor and that Stenger really wanted Rallo's Cardinal Creative Consulting to win a consulting contract through the Port Authority. Stenger told Sweeney to make it a $100,000 contract. Sweeney helped get CCC's bid selected by the Port Authority board. [redacted] it

was not a fair bidding process, but she was directed by Stenger to give it to Rallo because of his donor relationship.

c. Later, in Stenger's office, Stenger told Sweeney he needed to get $30,000 to J[redacted] C[redacted], [redacted] "guy". Stenger followed up with Sweeney several times, asking if she had figured out a way to get C[redacted] the money. Sweeney decided the best way to get C[redacted] the money was to add him to the CCC consulting contract. There was no expectation C[redacted] was going to do actual work for the money. Sweeney did not tell the SLCPA board that Stenger told Sweeney to select CCC, and Sweeney did not tell the SLCPA board that Stenger told her to get $30,000 to C[redacted].

d. When the media (St. Louis Post-Dispatch) began asking questions about the CCC contract, Stenger sent his media people to Sweeney to reiterate what to say. CCC's hiring of Montel Williams was the important message emphasized to Sweeney. Sweeney followed that direction even though she knew it was not true.

9. On June 23, 2018, the St. Louis Post-Dispatch printed an article titled "Documents raise questions about St. Louis Economic Development Partnership bidding procedures", by Jacob Barker. The article detailed the communications between John Rallo and Sheila Sweeney. Based on text messages reviewed by the FBI, it appears the newspaper reached out to various people, including Stenger and Sweeney in the days leading up to the article, attempting to get comments from them.

a. In a June 16, 2018 text message from Stenger's telephone, [redacted] Stenger wrote to Sweeney, "Please don't talk to him (Barker) till we talk and let's review his questions together." Sweeney responded one minute later, "Will do. And i don't plan

to talk to him. But once i have the questions I'll let you know. Nothing good can come of talking to him."

b. In a group text message on June 23, 2018 after the online article release but before the print article, Stenger was one of several individuals exchanging text messages in a group text thread. In response to the article being a campaign piece for Stenger's opponent, Stenger texted, "Yeah. It's basically defamatory." St. Louis Economic Development Partnership Vice President of Marketing and Communications, Katy Jamboretz, in the text communications thread, wrote, "It would substantially help our case if we can send him the Sheila/Steve Grelle email that says don't treat John Rallo any different than any other person." [redacted] this information from the text message to not treat Rallo differently was based on a different deal than the Cardinal Creative deal. On the Cardinal Creative deal, which is what the newspaper was asking about at the time, Rallo was treated differently because he was a donor and Stenger instructed Sweeney to get Rallo the contract.

10. There have been allegations of Stenger requiring campaign contributions before signing contracts or directing SLCPA contracts to large donors.

a. St. Louis Post-Dispatch printed an article dated March 13, 2017 titled "Meet the low-profile group that wields big power in St. Louis County". The article describes how the St. Louis County Port Authority's actions "don't ultimately go back to a legislative body – in this case, the St. Louis County Council – for final approval. It doles out millions of dollars a year in grants and contracts, one of which was awarded without other bids, possibly in violation of state statute." The article then discussed a $50,000 contract with Clayton-based Blitz, Bardgett and Deutsch for legal services related to a project. In

December the SLCPA increased the amount to $75,000. Bob Blitz, according to the article, wrote a $12,500 check in January 2017 and made an $8,000 donation in 2016 to Stenger's campaign account. The article wrote "Stenger said he had no role in the contracts and noted that the port authority board members were all appointed by former county executives. 'I played no role – directly or indirectly – in the port authority board's decision to hire Blitz, Bardgett, & Deutsch to handle these legal matters. I have no supervisory authority over the port authority, its board, its management or individuals hired by it.'" Based upon information received by [redacted] these public statements were false.

b. A text thread was reviewed as part of a forensic examination of Sheila Sweeney's cellular phone. Several people were on the thread, including Sweeney and Stenger. The substance of the texts is deciding how to respond to a newspaper request for information regarding the hiring of [redacted] On March 9, 2017, Stenger, using telephone [redacted], sent the text, "I think this would be my response," followed by, "I played no role directly or indirectly in the decision to hire Attorney [redacted] or his firm in these matters. I have no supervisory authority over the organization(s) or the individuals mentioned." Other individuals offered suggestions about how to respond.

c. [redacted] advised this statement by Stenger was not true. Stenger wanted the Economic Partnership to hire [redacted]; he wanted [redacted] hired because he was a close friend and political donor to Stenger.

11. Stenger told Sweeney that John Rallo was a member of the "$10,000 Club", who were donors who had given Stenger $10,000 or more annually. Stenger told Sweeney Rallo wanted to develop property owned by the St. Louis County Land Clearance for Redevelopment

Authority in Wellston, and Stenger wanted Rallo to get the contract. Sweeney helped Rallo with the bidding process for two separate pieces of land. Sweeney gave Rallo her personal email address to communicate with her so other people would not know she was reviewing Rallo's bids before Rallo formally submitted them. Rallo's company, Wellston Holdings, was the highest bidder on one contract, which he won. Sweeney did not tell the Land Clearance for Redevelopment Authority board that Stenger directed Sweeney to give Rallo the land contracts.

12. [redacted]

13. Stenger rarely came to the office in the months leading up to the November 6, 2018 County Executive election. On or about September 17, 2018, Stenger had a meeting at his residence. Bill Miller was present for this meeting. Miller had several questions to ask Stenger

about St. Louis County matters. When asked a question by Miller, Stenger yelled at Miller, stating, "I'm over here trying to run an election, trying to fucking raise money." Stenger then said he had "gotten calls all fucking day – [ ], [redacted]" The FBI assesses Stenger was frustrated because [redacted], a donor, was pressuring Stenger for updates on the rezoning issue. Miller repeatedly offered to handle the [redacted] relationships, including working directly with [redacted] and the various intermediaries in the bribe payment. Stenger declined the offer, saying he would handle it himself. A review of Stenger's telephone toll records on telephone [redacted] identified five text messages between [redacted] and Stenger on September 13-14, 2018 and a telephone call from Stenger to [redacted] on September 17, 2018, which lasted one minute and 47 seconds.

14. Stenger was asked on or about September 24, 2018 the percentage probability of [redacted] voting for the [redacted] Stenger responded, "About a hundred." Miller then stated, "This deal's getting done." Stenger replied, "Yeah! I think so! Let's just say they're talking [redacted] language." [redacted] have donated over $78,000 to Stenger's campaign, both before and after these text messages and telephone calls. On the date of this application the [redacted] had not taken place based on multiple, conflicting Port Authority Boards had not voted to approve the plan that would push it to a Council vote.

15. The FBI has debriefed additional people with knowledge of the individuals discussed throughout this affidavit. Their accounts of the "pay to play" politics under Stenger are consistent with the information reported herein from [redacted]

[redacted]

16. Court ordered Pen Registers on the subject cellular telephone, up to the current date, reveal that Stenger has regular telephone conversations and text messaging with a number of political donors who have current contracts with St. Louis County and the St. Louis County Port Authority.

17. [redacted] The most recent cellular telephone on Stenger's account is described as an "iPhone X Silver 256 GB", with serial number G6TWRPFBJCL7, purchased on July 22, 2018, attributed to telephone [redacted].

18. Based on my training and experience, I know that text messages sent between Steve Stenger and others, as well as email communications, are likely stored on the Apple telephone used by Stenger.

TECHNICAL CONSIDERATIONS

19. Based on my knowledge, training, and experience, as well as the experience of agents and investigators with specialized training involving cellular telephones and digital evidence, I know the following information concerning electronic devices: cellular telephones have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device. Phones create and keep log files associated with calls and text messages sent from and received by the device. I know that electronic devices can store

information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for lengthy periods of time on the device. This information can sometimes be recovered with forensics tools.

20. The FBI employs personnel with specialized knowledge, training and experience relating to computer and digital evidence, including evidence located on cell phones. Based on my knowledge, training and experience, and the knowledge, training and experience of law enforcement personnel involved in computer and digital forensics, I am aware of the following factors and considerations that may be pertinent:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. In addition to enabling voice communications, wireless telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing

names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and email; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

c. Electronic devices, such as cell phones, can store information for long periods of time. This information can sometimes be recovered from the device using forensic examination tools.

21. This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described herein, but also forensic evidence that establishes how the cell phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device, to include the text messages listed above and other related messages. Cell phones typically keep log files of calls and messages received and made from the device. These log files include the phone numbers called and received. The log files can stay on the device for long periods of time.

22. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. Specifically, there is reason to believe, based on the way that data is stored on cellular phones, that the incriminating text messages and contact history identified from the Pen Register data and cooperating witnesses described above related to Steven Stenger will also be contained on Stenger's cellular phone itself.

23. Additionally, based on my training and experience, I know that those who have committed crimes often delete incriminating evidence from their phones.

24. Based on my knowledge, training, and experience, as well as the experience of agents and investigators with specialized training involving cellular telephones and digital evidence, I know the following information concerning electronic devices: an iPhone is a high-end cellular telephone that combines the function of a personal digital assistant and a mobile phone. This includes the ability to communicate with other cell phones by using a text-messaging feature, email, or an Internet-based instant messaging application. Most smartphones also have the ability to connect to the Internet via Wi-Fi and mobile broadband access. I know from my training and experience that cell phones, including smartphones, are capable of storing large amounts of data, including call histories (showing the date, time, and destination/origin phone number dialed), emails, and message content of texts placed/received. Cell phones are relatively small, are easily concealed, and are frequently carried on someone's person or in their vehicle.

25. Obtaining cellular telephone records stored in cellular telephones may be helpful to law enforcement in many ways, including the following: identifying suspects, co-conspirators, or persons involved in or related to criminal activity; identifying victims; helping to establish a timeline of events surrounding criminal activity; and documenting contact between co-conspirators.

26. Specialized software and computer hardware can be used to examine the contents of mobile phone and smartphones. I know this software is capable of retrieving call history, text message history, and details, pictures, and videos from numerous types of mobile phones and smartphones. In some cases, the software is able to retrieve previously stored data even after a user has deleted it from the phone's memory.

27. Searching cell phones, and electronic storage devices is a highly technical process that requires specific expertise and specialized equipment. There are so many types of electronic hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search of every possible electronic device and system. In addition, it may also be necessary to employ or consult with personnel who have specific expertise in the type of electronic device or software application or operating system being searched:

> Searching electronic devices requires the use of precise, scientific procedures that are designed to maintain the integrity of the evidence and to recover "hidden" erased, compressed, encrypted, or password-protected data. Electronic hardware and software may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since electronic data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted. The volume of data stored on many electronic devices will typically be so large that it will be highly impractical to search for data during the execution of a search warrant; and users of electronic devices can attempt to conceal data within the devices through a number of methods, including the use of innocuous or misleading filenames and extensions, or by employing encryption or data-wiping software. Therefore, a substantial amount of time is necessary to extract and sort through data found on electronic devices to locate any data that may be concealed or encrypted and to determine what data constitutes evidence, fruits, contraband or instrumentalities of a crime.

27. The search procedure of electronic data contained in the hardware and software of the cell phone described in Attachment B and seized pursuant to this warrant may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. on-site triage to determine what, if any, peripheral devices or other electronic devices have been connected to the seized device;

b. a preliminary scan of image files contained on the devices to help identify relevant evidence, the known victim, or any potential victims, as well as a scan for encryption software;

c. on-site forensic imaging of devices that may be partially or fully encrypted, in order to preserve unencrypted electronic data that may, if not immediately imaged on-scene, become encrypted and accordingly unavailable for examination; such imaging may require several hours to complete and require law enforcement agents to secure the search scene until that imaging can be completed;

d. examination of all of the data contained in each device's hardware, software, or memory storage to view the data to determine whether that data falls within the items to be seized as set forth herein;

e. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not evidence of the offenses specified above);

f. surveying various file directories and the individual files they contain;

g. opening files in order to determine their contents;

h. scanning storage areas;

i. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and

j. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

28. I am aware that individuals often keep their cell phones on their person. Today, many people's cell phones are some form of "smart phone" which has the capability of connecting to the Internet. As noted above, any device that can connect to the Internet and transmit commands could have been used to send texts, emails, and access other online accounts, including submitting bids. For these reasons I seek permission to search the person of Steven Stenger identified in Attachment A for the information described in Attachment B.

Biometric considerations

29. Because the cellular telephone that is authorized to be searched under this warrant is an iPhone, Apple brand device, for the reasons that follow, this warrant application seeks Court permission for law enforcement to cause Steven Stenger to press his thumb and/or fingers to the "Touch ID" area of the phone, or use facial recognition features to unlock and unencrypt the device so that it can be forensically examined.

30. I know from my training and experience, as well as from information found in publicly available materials including those published by Apple, that some models of Apple devices such as iPhones offer their users the ability to unlock the device via the use of a fingerprint or thumbprint (collectively, "fingerprint") or by enabling the phone to scan the image of a person's

face in lieu of a numeric or alphanumeric passcode or password. This feature is called Touch ID Similarly, an Apple phone may also use a biometric software application to identify and verify a person by analyzing the unique features of their face. This feature is referred to as facial recognition a/k/a Apple Face ID.

31. Beginning with the release of Apple's iOS 8 operating system in September 2014, Apple no longer has a key to decrypt these devices. Thus, even with a properly authorized search warrant to gain access to the content of an iOS device, there is no feasible way for the government to search the device. I know from my training and experience and my review of publicly available materials published by Apple that those Apple devices can enable what is referred to as "Touch ID," a feature that recognizes up to five fingerprints designated by the authorized user of the iPhone. A Touch ID sensor, a round button on the iPhone, can recognize fingerprints. The fingerprints authorized to access the particular device are a part of the security settings of the device and will allow access to the device in lieu of entering a numerical passcode or longer alpha-numerical password, whichever the device is configured by the user to require. The Touch ID feature only permits up to five attempts with a fingerprint before the device will require the user to enter a passcode. Furthermore, the Touch ID feature will not substitute for the use of a passcode or password if more than 48 hours have passed since the device has been unlocked; in other words, if more than 48 hours have passed since the device was accessed, the device will require the passcode or password programmed by the user and will not allow access to the device based on a fingerprint alone. Similarly, Touch ID will not allow access if the device has been turned off or restarted, if the device has received a remote lock command, or if five attempts to match a fingerprint have been unsuccessful. For these reasons, it is necessary to use the fingerprints, thumbprints, and facial recognition of Steven Stenger to attempt to gain access to the Apple device

described in this warrant. The government may not be able to obtain the contents of the Apple devices if Steven Stenger's fingerprints, thumbprints, and facial recognition are not used to access the Apple devices by depressing them against the Touch ID button. Although I do not know which of the ten finger or fingers are authorized to access on any given Apple device and only five attempts are permitted, I know based on my training and experience that it is common for people to use one of their thumbs or index fingers for Touch ID, and in any event all that would result from successive failed attempts is the requirement to use the authorized passcode.

32. If a user enables Touch ID on a given Apple device, he or she can register up to 5 fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) found at the bottom center of the front of the device. In my training and experience, users of Apple devices that offer Touch ID often enable it because it is considered to be a more convenient way to unlock the device than by entering a numeric or alphanumeric passcode or password, as well as a more secure way to protect the device's contents. This is particularly true when the user(s) of the device are engaged in criminal activities and thus have a heightened concern about securing the contents of the device.

33. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and facial recognition technique may be used instead. Similarly, in some instances a password or passcode. These circumstances include: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the

device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; and (3) five unsuccessful attempts to unlock the device via Touch ID are made.

34. The passcode or password that would unlock the iPhone escribed herein is not known to law enforcement. Thus, it will likely be necessary to press the user's finger(s) to the device's Touch ID sensor in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. It may also be necessary to hold the phone up to the user's face to recognize the biometric features and unlock the phone. Attempting to unlock the relevant Apple device(s) via Apple Face ID or Touch ID with the use of the fingerprints of the user(s) is necessary because the government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant pursuant Rule 41 (e)(2)(B), which would permit a search of the individual identified in attachment A and the seizure and examination of the Device in attachment B consistent with the warrant. Upon receipt of the Device, government-authorized persons will review that information to locate the items described Attachment B. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium that might expose many parts of the device to human inspection in order to determine whether it is evidence described by this warrant.

CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) &

(c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

37. The foregoing has been reviewed by Hal Goldsmith, Assistant United States Attorney, U.S. Attorney's Office, Eastern District of Missouri.

REQUEST FOR SEALING

38. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

Andrew R. Ryder, Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on the 20th day of March, 2019.

HONORABLE SHIRLEY P. MENSAH
United States Magistrate Judge

ATTACHMENT A

The person to be searched is Steven Stenger (the "SUBJECT PERSON"), who resides at 336 N. Forsyth Blvd., St. Louis, Missouri. The SUBJECT PERSON is a 47 year-old white male, standing approximately 5 feet 10 inches tall, and weighing approximately 200 pounds. The SUBJECT PERSON is depicted in the photograph below:

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, in any format or medium, which constitute evidence, instrumentalities, and fruits of the criminal violations of 18 U.S.C. § 666, § 1343, and §1951 and involve Steven Stenger, and others from October 23, 2014, through the time of the execution of this warrant that may be deemed instrumentalities, fruits, or evidence of the aforementioned crimes to include:

1. The cellular phone, that being an Apple iPhone X, serial number G6TWRPFBJCL7 with associated phone number [redacted]. (The Device)

2. For the Device, all records and information to include:

   a. Call Logs showing numbers called and received, to include deleted logs;

   b. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

   c. Internet browsing history, including records of Internet Protocol addresses used; records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

   d. Photographs, videos, and other forms of media documenting the events that are the subject of this warrant.

   e. Any and all contact lists, address books, in whatever form regarding coconspirator

contact information, to include deleted information.

f. all bank records, checks, credit card bills, account information, and other financial records.

g. Text message records, including the content of messages as well as any logs showing text messages sent and received, to include deleted information

h. Any and all documents, notes, and records, including e-mail correspondence in whatever form, including digital, relating to the matters set forth in the attached Affidavit, to include deleted information

i. Any and all documents, notes, and records relating to the ownership and usage of the cell phone being searched

j. Any and all contact lists, address books, in whatever form regarding coconspirator contact information, to include deleted information

3. During the execution of this search warrant, law enforcement personnel are authorized to depress the fingers and/or thumbprints of Steven Stenger onto the Touch ID sensor of any Apple iPhone with Touch ID, and or initiate facial recognition a/k/a Apple Face ID feature belonging to this individual for the purpose of attempting to unlock the device via Touch ID or facial recognition in order to search the contents of the phone as authorized by this warrant

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.