AUSA: Robert White Telephone: (313) 226-9100

AO 106 (Rev. 04/10) Application for a Search Warrant Special Agent: Nick Jones, HSI Telephone: (619) 247-8315

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 69951 Wildflower Lane, Bruce Township Michigan 48065 (More fully described in Attachment A)	Case: 2:22−mc−51755-1 Assigned To : Berg, Terrence G. Assign. Date : 11/28/2022 In re: SEALED MATTER (MAW)

APPLICATION FOR A SEARCH WARRANT

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 Eastern District of Michigan, there is now concealed *(identify the person or describe the property to be seized)*:

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.§§ 1030, 2511	Computer hacking and unlawful interception of electronic communications
18 U.S.C.§§ 2512, 371	sale and advertising of unlawful interceptions and conspiracy to do the same

The application is based on these facts:

See attached AFFIDAVIT.

☐ Continued on the attached sheet.

☐ Delayed notice _____ 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.

Nick Jones

Applicant's signature

Nick Jones, Special Agent, HSI

Printed name and title

Sworn to before me and signed in my presence and/or by reliable electronic means.

Date: November 28, 2022

Elizabeth A. Stafford

Judge's signature

City and state: Detroit, MI

Hon. Elizabeth A. Stafford U. S. Magistrate Judge

Printed name and title

AFFIDAVIT

I, Nick Jones, being duly sworn, hereby depose and state as follows:

EXECUTIVE SUMMARY

1. This affidavit is in support of an application by the United States of America for a search warrant for 69951 Wildflower Lane, Bruce Township, Michigan 48065 (the "SUBJECT PREMISES"), as described in Attachment A, to search for and seize items that constitute evidence of violations of Title 18, United States Code, Sections 1030 (computer hacking), 2511 (unlawful interception of electronic communications), 2512 (sale and advertising of unlawful interception devices), and 371 (conspiracy), as well as fruits of a crime, other items illegally possessed, and property designed and intended for use, and used in committing a crime, as described in Attachment B.

2. As described below, the SUBJECT PREMISES is a single-family residence where public records indicate that Bryan FLEMING lives with his wife and son. Since at least 2016, FLEMING, sometimes through his company Fleming Technologies, LLC, has owned and operated the website pcTattletale.com, which markets and distributes software that enables pcTattletale customers to covertly monitor the cell phones and computers of unwitting individuals once the customer installs the pcTattletale software on the target device without the device user's knowledge. Business records and Internet Protocol (IP) addresses registered to the SUBJECT

PREMISES indicate that FLEMING has operated pcTattletale.com from his home since at least 2016.

3. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of victims; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth every fact that I or others have learned during this investigation. All dates, times, and amounts discussed herein are approximate.

EXPERIENCE & TRAINING

4. I am a Special Agent employed by United States Immigration and Customs Enforcement, Homeland Security Investigations (HSI) and have been so employed since 2004. I am currently assigned to HSI's San Diego Cyber Intrusion Group. I have a Bachelor of Arts Degree in Political Science from the University of California, Los Angeles. I am a graduate of the Criminal Investigator Training Program and the Immigration and Customs Enforcement Special Agent Training Program, at the Federal Law Enforcement Training Center. I have completed Network + and Global Information Assurance Certification Security Essentials Certification (GSEC) training.

As a member of the Cyber Intrusion Group, I investigate cybercrimes, such as computer intrusions (commonly referred to as hacking), unlawful interception of electronic communications, and Internet fraud and financial crimes. Based on my training and experience, I am familiar with the manner in which persons engaged in cybercrimes operate; the manner in which cybercrimes are perpetrated; certain techniques, methods, or practices commonly used by persons engaged in cybercrime activity; and indicia of cybercrime activity. This training and experience form the basis for opinions I express below.

STATEMENT OF PROBABLE CAUSE

A. *Overview*

5. In June 2021, I initiated an investigation into the unlawful sale and use of software applications that allow users to covertly and remotely monitor a victim's cell phone or computer. These applications are commonly known as "stalkerware" because of their tendency to be used by customers wishing to spy on an intimate partner's cell phone or computer without the partner's knowledge or consent. Typically, users will purchase a stalkerware application from a company via the company's public-facing website, secretly install the application on the victim's cell phone or computer, and then log into a different, client-facing website, which allows the customer to remotely monitor the victims' devices. In general, these stalkerware applications can allow a person to monitor and review a victims' text messages, phone calls, internet browsing activities, photographs, social media content, and geographic location data. In some

cases, the stalkerware can also remotely turn on the microphone and/or camera of a victim's device.

6. My early investigation revealed that there were over one hundred different websites selling stalkerware applications. I noticed that some of the sellers were advertising the applications for use in monitoring minor children's or employees' phones, which is often legal. I also saw that some sellers were specifically advertising and marketing the software applications for use in surreptitiously spying on spouses and partners, which is not legal. The investigation identified the website www.pctattletale.com as selling stalkerware that was directly or indirectly marketed for use in unlawful spying on spouses or partners.

7. As described below, records obtained during this investigation indicate that Bryan FLEMING is the owner of pcTattletale and resides at the **SUBJECT PREMISES**. According to public records, FLEMING resides at the **SUBJECT PREMISES** with his wife and son and has lived there since approximately November 2008. Records described below show that FLEMING uses the **SUBJECT PREMISES** to support and operate pcTattletale.com. I verified that the website was active as of November 14, 2022, and HSI special agents from the Detroit field office observed FLEMING entering the **SUBJECT PREMISES** on November 7, 2022.

8. In support of the investigation into FLEMING and pcTattletale, the government has obtained the following search warrants:

a. On February 3, 2022, United States Magistrate Judge Mitchell D. Dembin, of the Southern District of California, signed and approved a search warrant, 22MJ406, for Liquid Web Inc, for data and records regarding its hosting of pcTattletale's website and email services.

b. On July 15, 2022, United States Magistrate Judge Daniel E. Butcher, of the Southern District of California, signed and approved a search warrant, 22MJ2551, for Google LLC, for Gmail and Google Drive data and records associated with the Google account bfleming98@gmail.com. These records include both email correspondence and pcTattletale records that were stored, or archived, in Google Drive's cloud storage.

9. In support of the investigation into FLEMING and pctattletale.com, the government has also reviewed both the active pcTattletale.com website, as well as archived records from the website. HSI has also undertaken undercover communications with FLEMING, both as a marketing affiliate and as a customer, as well as gathered business records for pcTattletale from third-party businesses like PayPal and Citizens Bank.

10. As further described below, this evidence shows that FLEMING knowingly markets and distributes pcTattletale as a means for adults to surreptitiously spy on other, nonconsenting adults' electronic devices (e.g., cell phones and computers) and electronic communications and offers his customers guidance on how to install pcTattletale's software on victims' electronic devices without with their authorization.

Records further show that FLEMING and pcTattletale have offered these surveillance tools and services to spy on intimate partners since at least 2016.

B. *The pcTattletale Website*

11. The domain name "pctattletale.com" was registered in 2002 and the Internet Archive (aka the "Wayback Machine") has archived copies of the pcTattletale.com website dating back to July 15, 2003. Archived images of the website show that, throughout its existence, pcTattletale.com has marketed tools and services for spying on cell phones and computers. For the first ten years, archived copies of the website show it was marketed to parents as a means of monitoring minor children's online activities. These records are consistent with pcTattletale's own website (https://www.pctattletale.com/about.php) (last accessed on Nov. 4, 2022), which states that FLEMING and a second individual, D.S. created the website in 2002 to help parents monitor children's online activities and that FLEMING took exclusive control over the company in 2011. According to the website, FLEMING, by and through Fleming Technologies, LLC, operates pcTattletale "out of Detroit, Michigan, to this day." (The website does not provide a street address, but public records show that the **SUBJECT PREMISES** is in a Detroit suburb.) The website describes pcTattletale as "a virtual company, its workforce and infrastructure spread out around the entire planet. pcTattletale is being actively developed and improved on almost every day."

12. In 2012, archived copies of the pcTattletale website show that pcTattletale began marketing its surveillance tools to monitor both children and adult employees.

(Previously, archived copies of the website's landing page indicate the tools were marketed only to monitor children.) Seized emails further show that, since at least 2016, FLEMING and pcTattletale have knowingly assisted customers seeking to spy on nonconsenting, non-employee adults.

13. On November 3, 2021, and again on November 14, 2022, I reviewed the pcTattletale.com website. My review of the website revealed that the website's landing page (www.pctattletale.com) advertises a product called "pcTattletale Computer and Device Recorder" ("pcTattletale"), which it touts as the "#1 Employee & Child Monitoring Software." The landing page says, "pcTattletale is child monitoring software. It lets you see what your kids are doing online. It runs invisibly in the background of their devices and can not [sic] be detected. They will have no idea you are able to see everything they do. PcTattletale is the only solution that makes 'YouTube' like videos of their every tap or click. Just watch the recordings from your phone or computer using your secure pcTattletale account as they live their secret online lives." The website currently markets pcTattletale's services for a cost of approximately $99/year.

14. The pcTattletale website landing page includes a footer that reads:

> pcTattletale SOFTWARE INTENDED FOR LEGAL USE ONLY. Installing the Licensed Software onto the device you do not possess monitoring rights may go against the Laws of your country or region. Violation of the law's requirements would be liable to severe monetary and criminal penalties.

> Please consult your own legal advisor for professional opinions on the legality of using this Licensed Software in the way you intend to use. You take full responsibility for downloading, installing, and using it. pcTattletale shall not be responsible if you choose to monitor a device without being permitted to; nor can pcTattletale provide legal advice on the use of the monitoring software.

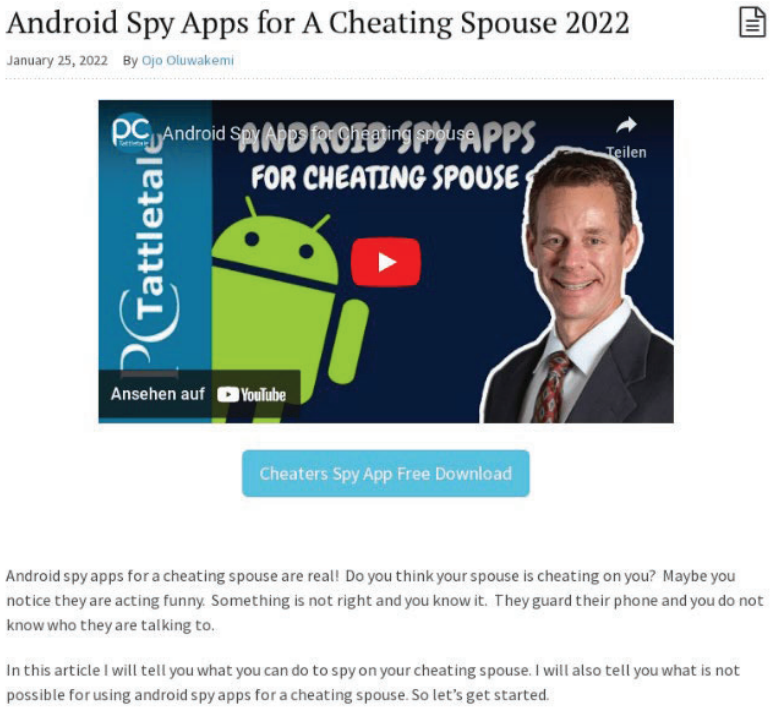
15. The pcTattletale website also has a webpage (https://www.pctattletale.com/terms.php) (last accessed November 4, 2022) entitled, "pcTattletale Terms and Conditions" that outlines pcTattletale's "End User License Agreement" ("EULA") between pcTattletale and its customers. According to the webpage, the ULA "CONSTITUTES A BINDING AGREEMENT BETWEEN YOU THE PURCHASER, AND/OR ANY OTHER THIRD PARTY USING THE SOFTWARE ("USER"), AND FLEMING TECHNOLOGIES, LLC. ("FTC")." According to the EULA:

> BY ACCEPTING THIS AGREEMENT, YOU AGREE TO ONLY INSTALL THIS SOFTWARE ON A DEVICE OR DEVICES OWNED BY THE USER. USER ALSO AGREES TO INFORM ANY PERSON(S) WHO USES A DEVICE WITH THE SOFTWARE INSTALLED OF THE PRESENCE OF THE SOFTWARE. FAILURE TO COMPLY MAY RESULT IN YOU BREAKING STATE AND FEDERAL LAWS.

16. Despite pcTattletale's EULA and landing page describing pcTattletale as being intended solely for lawful monitoring, the website landing page advertises that, "pcTattletale has been developed for over 15 years and has helped thousands of *spouses*, family's [sic], and employers just like you." (Emphasis added.) Additional pages on the pcTattletale website also explicitly discuss spying on adult partners without their knowledge or consent. As of November 2, 2022, these additional pages, which are available via hyperlinks from the pcTattletale landing page, include blog posts entitled, "Android Spy Apps for a cheating Spouse," "Catch Your Boyfriend Cheating App," and "Hidden Spy Apps for Android."

17. Examples of past and present language from these pcTattletale blog posts include the following:

a. As of November 2, 2022, the URL https://www.pctattletale.com/blog/1834/android-spy-apps-cheating-spouse/ is a blog post that is dated January 25, 2022, entitled "Android Spy Apps for a Cheating Spouse 2022." The blog post begins, "Android spy apps for a cheating spouse are real!" and continues, "In this article I will tell you what you can do to spy on your cheating spouse. I will also tell you what is not possible for using android spy apps for a cheating spouse." The blog post also includes an image and embedded link to a YouTube video that advertises these surveillance services and features FLEMING's likeness (based on my review of and comparison to FLEMING's U.S. passport photo):



Android Spy Apps for A Cheating Spouse 2022

January 25, 2022 By Ojo Oluwakemi

Android Spy Apps for Cheating Spouse

Teilen

Ansehen auf YouTube

Cheaters Spy App Free Download

Android spy apps for a cheating spouse are real! Do you think your spouse is cheating on you? Maybe you notice they are acting funny. Something is not right and you know it. They guard their phone and you do not know who they are talking to.

In this article I will tell you what you can do to spy on your cheating spouse. I will also tell you what is not possible for using android spy apps for a cheating spouse. So let's get started.

b. An archived version of the same URL (https://web.archive.org/web/20210123141821/https://www.pctattletale.com/blog/1834/android-spy-apps-cheating-spouse/) is a blog post, dated January 9, 2021, entitled "Android Spy Apps for A Cheating Spouse 2021." The post echoes the subsequent January 25, 2022 blog post and elaborates, "Your first thought is probably something like this 'How can I send them a text message or something and trick them into putting the spy software on their phone?'. The idea of course is that you want to remotely slip the spy app on their phone without them knowing. Not gonna happen. At pcTattletale we spent countless hours looking at every possible way to do this." The post goes on to explain some of the technical challenges with installing a spy app and concludes, "To catch a cheating spouse you will need to get a hold of their phone. You will need their

pass-code too to get into the phone. Using an android spy app like pcTattletale you can catch your cheating spouse without needing to root the device either."

c. The URL https://www.pctattletale.com/blog/3926/catch-your-boyfriend-cheating-app/ is a blog post that is dated January 7, 2022, entitled "Catch Your Boyfriend Cheating App." The post includes similar language to the two other posts (e.g., "Your biggest concern is probably just getting a hold of his phone to put a spy app on it that will catch him cheating on you. If he always has his phone on him this can be pretty hard. Plus you will need to know the unlock code to his phone."). This post also addresses the challenges of installing a spy app on iPhones, warning users that Apple's security had made it virtually impossible to spy on an iPhone, but offers the "tip" to "Try a computer based Catch Your Boyfriend Cheating App," which pcTattletale also markets.

C. *Undercover Activity*

18. As described herein, HSI has engaged in undercover communication with FLEMING in two ways: first, as an affiliate marketing partner and, second, as a customer. For context, businesses engaged in electronic commerce, or "e-commerce," sell goods and services over the internet. One of the marketing strategies employed by e-commerce sites to attract new customers, commonly referred to as "affiliate marketing," involves the e-commerce website paying a commission or fee to third parties that successfully direct customers to the e-commerce website. Depending on the agreement between the e-commerce website and the affiliate marketer(s) it engages

with, this fee or commission may depend on what type of action the prospective customer takes (e.g., merely visiting the website, signing up for a free account, or buying the actual service). To track which third-party affiliate referred which customer, and what fee or commission results from the referral, many e-commerce websites use an affiliate management service. In this case, pcTattletale has used at least two affiliate management services: ClickBank and LinkConnector.

19. According to records obtained from LinkConnector, pcTattletale.com had more than 45 active affiliate advertisers registered with LinkConnector in 2021. On December 2, 2021, I completed a review of records provided by LinkConnector for an account I believed to be used by FLEMING for pcTattletale.com. According to LinkConnector's business records, the account was registered to FLEMING and Fleming Technologies LLC, located at 69951 Wildflower, Bruce Township, MI (the **SUBJECT PREMISES**), and listed the phone number (248) 974-6876 (T-1).[1]

20. On November 3, 2021, acting in an undercover capacity, I visited pcTattletale.com and selected an option on the site to become an affiliate marketer. The website then directed me to ClickBank, where I established an undercover account. ClickBank, in turn, provided me with an affiliate account and username to be used to

[1] While the mailing address for the **SUBJECT PREMISES** is 69951 Wildflower Ln, Bruce Township, MI 48065, FLEMING appears to regularly omit the "Ln" or "Lane" designation and instead identifies the address as 69951 Wildflower [sic], Bruce Township, MI." There are no public records indicating a different 69951 Wildflower street address in Bruce Township than the one where FLEMING resides. Accordingly, this affidavit treats the two addresses as the same.

market pcTattletale.com. I then returned to pcTattletale.com and, using my ClickBank username, completed the process of becoming a pcTattletale.com affiliate. Once accepted as a pcTattletale.com affiliate, I received pcTattletale.com affiliate marketing materials. The materials included links and banners for me to use in digital advertising to direct customers to the pcTattletale.com website. I also received a pcTattletale.com promotional video explaining the pcTattletale product. The promotional video included a description of how the pcTattletale spy application can be used to catch a cheating spouse. The video stated that the pcTattletale software application is completely undetectable by the user of the phone, and that the application will allow someone to covertly see everything that is happening on the target cell phone, to include text messages.

21. Acting in an undercover capacity as a pcTattletale affiliate marketer, I had the following communications with FLEMING regarding pcTattletale:

a. On November 4, 2021, acting as a pcTattletale.com affiliate, I used the pcTattletale.com website to request marketing materials. On November 5, 2021, I received an email from support@pctattletale.com in which the sender, who identified himself as FLEMING, stated, "Did you sign up with ClickBank or LinkConnector? Glad to have you aboard. How do you plan on marketing? Maybe I can help you out. Bryan Fleming."

b. On November 6, 2021, I emailed FLEMING at support@pctattletale.com and told him that I had signed up through ClickBank and

planned to market the software as a tool to catch a girlfriend who cheats on you. The same day, FLEMING sent the following reply from support@pctattletale.com:

> Sounds good… If you need some banners made just send me the text and I can get some made for you. I upgraded your account to a paid $99 account. Feel free to try pcTattletale out and make some screen shots. https://www.pctattltale.com/members/ Let me know how it converts to you always looking for good feedback to make you guys more profitable.
>
> Bryan Fleming
>
> support@pctattletale.com

c. On November 9, 2021, I sent an email to FLEMING at support@pctattletale.com that stated, "yes thank you! You have banner to catch girlfriend I can use? Than[k] you friend!" The next day, I received an email from FLEMING at support@pctattletale.com that stated, "Here you go. There are a lot more women wanting to catch their man then the other way around 😊" Attached to the email were four banner images, on each of which was written either: "pcTattletale Cheating Husband? #1 catch a cheater spy app," "pcTattletale #1 Employee monitoring software," "pcTattletale Cheating Husband? #1 catch a cheater spy tracker," or "pcTattletale Husband Cheating? Best Catch a Cheater Spy App."

22. On January 20, 2022, acting in a different undercover capacity as a potential pcTattletale customer, I created a user account on pcTattletale.com, downloaded the pcTattletale app, and paid $99.99 for a subscription to monitor three

devices for one year. On January 26, 2022, I received the following email from info@pctattletale.com purporting to be from FLEMING:

> "Congratulations! You got pcTattletale recording your Android device.
>
> Every screen touch and their GPS location is secretly being recorded so you can see it.
>
> If your device is running a newer version of Android (7 or newer) make sure to turn off notifications and icons. Otherwise they will find pcTattletale and stop it from working.
>
> To turn off the notifications read this blog post:
>
> http://www.pctattletale.com/blog/1609/pc-tattletale-android-setup/ Look for the section called "Remove Android 7,8 & 9 Notifications and Popups".
>
> Samsung/Huawei phone users - Use the link above to disable additional warnings that these phones can cause. It is at the bottom of the article.
>
> . . .
>
> At your service,
>
> (a photograph of FLEMING)
>
> Bryan Fleming
>
> pctattletale.com

Suite #621

119 Church St.

Romeo, MI 48065[2]

23. Queries of law enforcement and internet databases and records, including usps.com, indicate that the address 119 Church St., Romeo, MI is assigned to a U.S. Post Office, from which I infer that "Suite #621" is, in fact, a P.O. Box within the U.S. Post Office located at this address. The Romeo, MI Post Office appears to be the Post Office closest to the **SUBJECT PREMISES**. Based in part on this evidence, I do not believe that FLEMING or pcTattletale operate out of this Romeo, MI address; rather, I believe it is more likely that FLEMING uses a P.O. Box at this Post Office to receive mail from pcTattletale customers.

24. On January 26, 2022, I installed the pcTattletale spy application on an undercover cellular telephone, using instructions from the website. Following the installation, I was able to login to the user dashboard to remotely monitor the device, to include seeing electronic communications, web browser activity, and location information.

25. On January 31, 2022, still acting in an undercover capacity, I sent an email to info@pctattletale.com that stated, "hello I already purchased this? I don't know why

[2] Pursuant to my search of FLEMING's Google account, discussed below, I am aware that this email that I received on January 26, 2022, while acting undercover as a customer, is the same or very similar to emails that FLEMING and pcTattletale regularly sent to new pcTattletale customers.

it is saying i didn't? Also I know my boyfriend is using the phone but nothing is showing up on the dashboard yet? help please!"

26. On February 1, 2022, I received the following email from FLEMING at support@pctattletale.com (emphasis added):

> Gigi, Yes you account is all set. With the Moto G were you able to load it with your computer? *I also have that same phone*. It will work without stopping if you can do it this way:
>
> http://www.pctattletale.com/blog/3462/install-android-with-computer/
>
> Bryan Fleming
>
> support@pctattletale.com

D. *Search Warrants for Electronic Records*

27. Public domain registration records for the domain pcTattletale.com show that it was created on November 7, 2002, and was assigned, as of November 2022, to an IP Address hosted by Liquid Web. Historical records known as passive DNS show that Liquid Web began hosting pcTattletale.com on approximately December 5, 2011. This timing is consistent with statements on the pcTattletale website, described above, indicating that FLEMING took exclusive control of pcTattletale in 2011. Based in part on these records, I believe that FLEMING has been the sole owner and operator of the pcTattletale.com website since 2012.

28. As mentioned above, on February 3, 2022, HSI obtained a search warrant for Liquid Web for data and records regarding its hosting of pctattletale.com. Subscriber and billing records for the pcTattletale.com Liquid Web account identified the account's subscriber as Bryan FLEMING, 69951 Wildflower, Bruce, MI, (the **SUBJECT PREMISES**) and listed his contact email as bfleming98@gmail.com.

29. An HSI forensic examiner helped me review the records provided by Liquid Web pursuant to this warrant. According to the forensic examiner, the Liquid Web pctattletale.com account was set up to automatically archive its electronic records, including email communications involving pctattletale.com email accounts, to a Google Drive folder. Based in part on this evidence and evidence that FLEMING used the email address bfleming98@gmail.com to further pcTattletale's business, HSI obtained a search warrant for the Gmail and Google Drive records associated with this Google account.

30. These searches revealed communications that indicated that pcTattletale.com customers were buying pcTattletale to spy on intimate partners, including the following examples:

a. On November 14, 2016, an individual with the email address [E.D.]@yahoo.com[3] wrote to jamie@pctattletale.com, in relevant part, "is it possible to

[3] This and other email addresses using brackets ([]) are redacted to preserve the user's privacy in the event this affidavit is unsealed and the account user is not charged or otherwise identified.

put this program on my husband's work computer from my home, remotely and anonymously? Or would I have to download it onto his work computer?"

b. On July 30, 2017, an individual with the email address [M.Z.]@yahoo.com wrote to jamie@pctattletale.com, in relevant part, "I don't think it is working on my husband's computer. It says on my dashboard that recording is paused until next restart. I have restarted his computer twice and still nothing. And how long is the delay from the clicks till I can see it on the recording. I rarely have the opportunity to have access to his computer. Was hoping to be finished by now."

c. On September 10, 2017, an individual with the email address [A.P.]@yahoo.com wrote to jamie@pctattletale.com, in relevant part, "Message: 4th time contacting you without any response. I have this on my boyfriend's android phone. Today recorded maybe 10 minutes and now its off. I needed to see his shit today but I wasn't able to and now hes probably out with his whore. I could've prevented this or left him but I need proof. How can I get proof if this doesn't work and no one will answer me back."

d. On November 18, 2017, an individual with the email address [S.H.]@yahoo.com wrote to jamie@pctattletale.com, in relevant part, "Also if there is a way to NOT let user know you are taking screen shot that would be helpful too. My husband knows when there is screen shot being taken as it beeps. He is now suspicious of something being on his phone. If these two bugs are worked out I think this product could be very successful."

e. On October 5, 2018, an individual with the email address [C.A.]@gmail.com wrote to bleming98@gmail.com, in relevant part, "I lost the download link to get it on my husband's phone and about how long will it take to install it so he doesn't notice." Two days later, FLEMING responded, "I would give your self about 1/2 hour. The software installs easily enough but there might be extra icons and pop ups you need to rid of. works best if you have your own phone to try it on first. Here are the instructions: http://www.pctattletale.com/blog/1609/pc-tattletale-android-setup/[.]"

f. On May 1, 2019, an individual with the email address [J.L.]@gmail.com wrote to bleming98@gmail.com, in relevant part, "Since im using my boyfriends card. I don't want him to see pc tattletale..you said it would cost 99$ To Change it to a different name ...where do I pay for that." The next day, FLEMING responded, "On our checkout page we have an option that does not say PC tattletale It will show up as a generic computer scan."

g. On May 13, 2020, an individual with the email [A.B.]@gmail.com wrote to bleming98@gmail.com, in relevant part, "I'm not able to use the application? I was so lucky to actually get my husbands phone while unlocked for 4 mins. I downloaded the app an[d] I got nervous an accidentally closed phone & it locked me out. The app is downloaded on his phone. But when I open my app it doesn't work bc it tells me to download the app on the target phone..Is there a way around this? Thanks."

h. On Oct 25, 2021, an individual with the email [B.P.]@aol.com wrote to blfeming98@gmail.com, in relevant part, "Hi Bryan, I have told Auslogics Boostspeed to ignore the proper folder on my husband's laptop, I have made exceptions in Malwarebytes and Windows Defender, but his computer is still going idle after about 1/2 hour, and I know that he's still on it. What else could cause this? I believe I have the latest version installed. I'm wondering if he figured out a way to make this happen? Could they do that? If so, how?"

i. On July 15, 2022, FLEMING received an email at bfleming98@gmail.com from email@pcTattletale.com referring to "Help Ticket (#2624)" with the message, "How do you say I installed it on my boyfriend's phone to see if he's cheating and did not copy. . . Copied the one I got off of his phone how do I fix this cuz I just installed it and copied it from his phone browser not mine."

31. I believe that these emails, together with the marketing materials discussed above, indicate that, since at least 2016, FLEMING and his company pcTattletale have knowingly helped pcTattletale customers gain unauthorized access to the devices and electronic communications of non-consenting adult victims that include intimate partners like spouses and boyfriends.

E. *The SUBJECT PREMISES*

32. While FLEMING used what appears to be a P.O. Box in Romeo, Michigan as pcTattletale's business address in the January 2022 email I received when I conducted an undercover purchase of pcTattletale's services, the business records

obtained in this investigation indicate that FLEMING operates pcTattletale and Fleming Industries LLC from his home at the **SUBJECT PREMISES**. I believe that FLEMING may have used the Romeo P.O. Box in his communications with individual customers because he wanted the company to seem like it had an official address and did not want these individuals to know his home address, whereas he did not have this concern about revealing his address to third-party business like LinkConnector, PayPal, and Citizens Bank.

33. Examples of the business records for which FLEMING has listed the **SUBJECT PREMISES** as pcTattletale's business address include the following:

a. As mentioned above, pcTattletale's EULA is between Fleming Technologies, LLC (rather than FLEMING individually) and the website's customers. LinkConnector records also show that FLEMING listed Fleming Technologies, LLC as the merchant-client for pcTattletale.com and the "pc Tattletale spy & mobile GPS tracker" ad campaign. Michigan Secretary of State online records show that, as of the company's most recent annual statement filed on October 18, 2022, Fleming Technologies, LLC is registered to FLEMING at 69951 Wildflower, Bruce Township, MI 48065 (the **SUBJECT PREMISES**). Earlier filings going back to at least 2016 also confirm that Fleming Technologies, LLC is registered to FLEMING at 69951 Wildflower, Bruce Township, MI 48065 (the **SUBJECT PREMISES**).

b. Records obtained from PayPal in late 2021 show that FLEMING created a PayPal account for "PC Tattletale" and the website

"http://www.pctattetale.com" on August 5, 2016, and registered the account to "PC Tattletale," 69951 Wildflower, Bruce, MI, US 48065 (the **SUBJECT PREMISES**), and listed the phone number (248) 974-6876 (T-1). PayPal records further show that the "PC Tattletale" PayPal account remained active through December 23, 2021, and had received a total of $613,987.81 as of that date. (Seized emails, including one described below, indicate that the "PC Tattletale" PayPal account remained active as of at least July 2022.) PayPal records also show that, between January 1, 2020 and December 23, 2021, the "PC Tattletale" PayPal account received approximately 4,807 transactions. Account records show that the "PC Tattletale" PayPal account was linked to a Citizens Bank Account ending in -9462.

c. Citizens Bank records show that an account ending in -9462, which is assigned to Fleming Technologies, was opened in October 2006 and remained active as of April 2022. The sole signatory to the account is listed as Bryan FLEMING, 69951 Wildflower Ln, Bruce Township, MI (the **SUBJECT PREMISES**). As of March 31, 2022, the account had a balance of $178.85.

d. Subscriber and billing records for the pcTattletale.com Liquid Web account identified the account's subscriber as Bryan FLEMING, 69951 Wildflower, Bruce, MI, (the **SUBJECT PREMISES**) as of February 2022.

e. Subscriber and billing records for the pcTattletale.com LinkConnector account discussed above show it was registered to FLEMING and his company Fleming Technologies LLC, located at 69951 Wildflower, Bruce Township,

MI (the **SUBJECT PREMISES**), along with the phone number (248) 974-6876 (T-1), as of December 2021.

f. LinkConnector records for FLEMING's pcTattletale.com account include IP login records. These records indicate that the IP address 68.61.87.216 (**IP-1**) accessed the pcTattletale.com LinkConnector account on November 21, 2021, November 24, 2021, and November 27, 2021. Comcast records for **IP-1** show that, on these dates (and at the times identified by LinkConnector), **IP-1** was assigned to Bryan FLEMING for service at 69951 Wildflower Ln, Bruce TWP, MI (the **SUBJECT PREMISES**).

g. According to the records provided by Google in response to the July 15, 2022 search warrant, FLEMING was actively using the "bfleming98" Google account as of the date of the warrant. Google's records, which list FLEMING as the account's subscriber and (248) 974-6876 (T-1) as the account's recovery cell phone, include log-in activity for the account going back to October 23, 2021. These log-in records indicate that:

i. Between October 23, 2021 and July 2, 2022, the account was accessed approximately 183 times from **IP-1**, often using what appears, based on Google's user information, to be an Apple computer.

ii. Between May 16, 2022 and July 15, 2022, FLEMING's "bfleming98" Google account was accessed 16 times from the IP address 47.50.92.54,

which is assigned to Spectrum (and for which HSI is awaiting subscriber records), using what appears to be an Apple computer.

iii. Between December 28, 2021 and July 6, 2022, the "bleming98" account was repeatedly accessed by IP addresses assigned to Verizon Wireless (and for which HSI is awaiting subscriber records), which suggests that these log-ins were from a mobile phone or tablet connected to a cellular network. The phone number (248) 974-6876 (T-1), which FLEMING provided to Google, PayPal, and LinkConnector, is assigned to Verizon Wireless (although HSI is still awaiting phone records for T-1 from Verizon).

h. Results from the search of FLEMING's Gmail account, bfleming98@gmail.com, included email correspondence with Ahrefs Ltd. ("Ahrefs"), a website analytics, marketing, and search engine optimization service provider.[4] These emails show that, in July 2022, FLEMING was using Ahrefs to promote the pcTattletale website and that a $99 monthly invoice, emailed to him on July 11, 2022, listed the customer as "Bryan Fleming, bfleming98@gmail.com, 66951 Wildflower Lane, Bruce, Michigan 48065" (the **SUBJECT PREMISES**). Seized emails also show that FLEMING used the "PC Tattletale" PayPal account (described above) to pay the invoice the same day.

[4] "Search engine optimization," sometimes referred to as "SEO," is a service that boosts a website towards the top of the results generated by a search engine like Google so that the client website gets more traffic.

34. On November 7, 2022, agents assigned to HSI's Detroit field office performed surveillance of the **SUBJECT PREMISES** and observed an individual matching FLEMING's appearance walking into the **SUBJECT PREMISES**.

35. Based on the evidence showing that FLEMING and pcTattletale are marketing and distributing software that surreptitiously monitors electronic communications on targets' phones and computers and requires customers (who, in some cases, would be coconspirators) to install this software with the device user's knowledge, and that FLEMING is operating this business from the **SUBJECT PREMISES**, I submit there is probable cause to search the **SUBEJCT PREMISES** for evidence of and relating to violations of 18 U.S.C. §§ 1030 (computer hacking), 2511 (unlawful interception of electronic communications), 2512 (sale and advertising of unlawful interception devices), and 371 (conspiracy).

36. The evidence described above shows that FLEMING is using email, cell phone service, Google Drive, YouTube, and the pcTatteltale.com website to advance pcTattltale's business operations. In addition, based on statements FLEMING has made on the pcTattletale.com website, as well as in YouTube videos that I have watched, FLEMING regularly tests pcTattletale on different types of cell phones and operates pcTattletale as a "virtual" company (i.e., one without a dedicated business space). It is therefore likely that FLEMING would need to have electronic storage and communication devices at the **SUBJECT PREMISES** to operate, distribute, and test the pcTattletale software.

37. IP log-in records for electronic accounts used by FLEMING to conduct and further pcTattletale's business show that **IP-1**, which is assigned to the **SUBJECT PREMISES**, has accessed both the "bfleming98" Google account and the pcTattletale LinkConnector account. These IP log-in records are consistent with the various other business records showing that FLEMING appears to operate pcTattletale from the **SUBJECT PREMISES**. Based on this evidence, I submit there is therefore probable cause to search electronic communication and storage devices like cell phones, tablets, and computers, as well as stand-alone storage devices like CDs, hard drives, and thumb drives, found within the **SUBJECT PREMISES** that are possessed or controlled by FLEMING.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

Computers, Tablets, and Electronic Storage Devices

38. With the approval of the Court in signing this warrant, agents executing this search warrant will employ the following procedures regarding computers and other electronic storage devices, including electronic storage media, that may contain data subject to seizure pursuant to this warrant.

Seizure and Retention of Instrumentalities

39. Based upon the foregoing, there is probable cause to believe that the subject premise is likely to contain computers, iPads, and electronic storage devices that may contain contraband and fruits of crime as provided at Rule 41(c)(2) of the Federal Rules of Criminal Procedure, or were used in committing crime as provided at Rule

41(c)(3), and are therefore instrumentalities of the enumerated offenses. If so, any such computers or electronic storage devices (collectively, "the subject devices") are subject to seizure, retention, and possible forfeiture and destruction.

40. The imaging and preliminary analysis of the subject devices to confirm their status as instrumentalities will be conducted within forty five (45) days of this warrant being signed. Seized items confirmed to be instrumentalities will not be returned and will be further analyzed as provided below. If the preliminary analysis, by definition an incomplete or partial analysis, does not confirm that a seized item is an instrumentality, the original item will be available to be reclaimed. An image of the subject devices will be retained and subjected to a complete forensic analysis, however, as provided below.

41. If the subject devices are retained as instrumentalities they will not be returned to the owner. The owner will be provided the name and address of a responsible official to whom the owner may apply in writing for return of specific data not otherwise subject to seizure for which the owner has a specific need. The identified official or other representative of the seizing agency will reply in writing. If the owner's request is granted, arrangements will be made for a copy of the requested data to be obtained by the owner. If the request is denied, the owner will be directed to Rule 41(g) of the Federal Rules of Criminal Procedure.

Identification and Extraction of Relevant Data

42. A forensic image is an exact physical copy of the hard drive or other electronic storage media. After obtaining a forensic image, the imaged copy will be analyzed to identify and extract data subject to seizure pursuant to this warrant. Analysis of the data following the creation of the forensic image can be a highly technical process requiring specific expertise, equipment, and software. There are thousands of different hardware items and software programs, and different versions of the same programs, that can be commercially purchased, installed, and custom-configured on a user's computer system. Computers are easily customized by their users. Even apparently identical computers in an office environment can be different with respect to configuration, including permissions and access rights, passwords, data storage, and security. It is not unusual for a computer forensic examiner to have to obtain specialized hardware or software, and train with it, in order to view and analyze imaged data.

43. Analyzing the contents of a computer or other electronic storage device, even without significant technical challenges, can be very challenging. Searching by keywords, for example, often yields many thousands of hits, each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant hit does not end the review process for several reasons. The computer may have stored metadata and other information about a relevant electronic record – e.g., who created it, when and how it was created or downloaded or copied, when it was last accessed, when it was last modified, when it

was last printed, and when it was deleted. Keyword searches may also fail to discover relevant electronic records, depending on how the records were created, stored, or used. For example, keywords search text, but many common electronic mail, database, and spreadsheet applications do not store data as searchable text. Instead, the data is saved in a proprietary non-text format. Documents printed by the computer, even if the document was never saved to the hard drive, are recoverable by forensic programs because the printed document is stored as a graphic image. Graphic images, unlike text, are not subject to keyword searches. Similarly, faxes sent to the computer are stored as graphic images and not as text. In addition, a particular relevant piece of data does not exist in a vacuum. To determine who created, modified, copied, downloaded, transferred, communicated about, deleted, or printed the data requires a search of other events that occurred on the computer in the time periods surrounding activity regarding the relevant data. Information about which user had logged in, whether users share passwords, whether the computer was connected to other computers or networks, and whether the user accessed or used other programs or services in the time period surrounding events with the relevant data can help determine who was sitting at the keyboard.

44. It is often difficult or impossible to determine the identity of the person using the computer when incriminating data has been created, modified, accessed, deleted, printed, copied, uploaded, or downloaded solely by reviewing the incriminating data. Computers generate substantial information about data and about users that

generally is not visible to users. Computer-generated data, including registry information, computer logs, user profiles and passwords, web-browsing history, cookies and application and operating system metadata, often provides evidence of who was using the computer at a relevant time. In addition, evidence such as electronic mail, chat sessions, photographs and videos, calendars and address books stored on the computer may identify the user at a particular, relevant time. The manner in which the user has structured and named files, run or accessed particular applications, and created or accessed other, non-incriminating files or documents, may serve to identify a particular user. For example, if an incriminating document is found on the computer but attribution is an issue, other documents or files created around that same time may provide circumstantial evidence of the identity of the user that created the incriminating document.

45. Analyzing data has become increasingly time-consuming as the volume of data stored on a typical computer system and available storage devices has become mind-boggling. For example, a single megabyte of storage space is roughly equivalent to 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is roughly equivalent to 500,000 double-spaced pages of text. Computer hard drives are now being sold for personal computers capable of storing up to 2 terabytes (2,000 gigabytes) of data. And, this data may be stored in a variety of formats or encrypted (several new commercially available operating systems provide for automatic encryption of data upon shutdown of the computer). The sheer volume of

data also has extended the time that it takes to analyze data. Running keyword searches takes longer and results in more hits that must be individually examined for relevance. And, once reviewed, relevant data leads to new keywords and new avenues for identifying data subject to seizure pursuant to the warrant.

46. Based on the foregoing, identifying and extracting data subject to seizure pursuant to this warrant may require a range of data analysis techniques, including the use of hashing tools to identify evidence subject to seizure pursuant to this warrant, and to exclude certain data from analysis, such as known operating system and application files. The identification and extraction process may take weeks or months. The personnel conducting the identification and extraction of data from the subject devices will complete the analysis within one-hundred twenty (120) days from the date this warrant is signed, absent further application to this court.

47. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

Cellular Telephones

48. It is not possible to determine, merely by knowing the cellular telephone's make, model and serial number, the nature and types of services to which the device is subscribed and the nature of the data stored on the device. Cellular devices today can be simple cellular telephones and text message devices, can include cameras, can serve as personal digital assistants and have functions such as calendars and full address books

and can be mini-computers allowing for electronic mail services, web services and rudimentary word processing. An increasing number of cellular service providers now allow for their subscribers to access their device over the internet and remotely destroy all of the data contained on the device. For that reason, the device may only be powered in a secure environment or, if possible, started in airplane mode which disables access to the network. Unlike typical computers, many cellular telephones do not have hard drives or hard drive equivalents and store information in volatile memory within the device or in memory cards inserted into the device. Current technology provides some solutions for acquiring some of the data stored in some cellular telephone models using forensic hardware and software. Even if some of the stored information on the device may be acquired forensically, not all of the data subject to seizure may be so acquired. For devices that are not subject to forensic data acquisition or that have potentially relevant data stored that is not subject to such acquisition, the examiner must inspect the device manually and record the process and the results using digital photography. This process is time and labor intensive and may take weeks or longer.

49. All forensic analysis of the data contained within any cellular telephone, and its memory cards, seized pursuant to this warrant will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

50. Based on the foregoing, identifying and extracting data from any cellular telephones and cellular telephone memory cards seized pursuant to this warrant may

require a range of data analysis techniques, including manual review, and, consequently, may take weeks or months. The personnel conducting the identification and extraction of data will complete the analysis within ninety (90) days, absent further application to this court.

Genuine Risks of Destruction of Data

51. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence.

PRIOR ATTEMPTS TO OBTAIN THIS EVIDENCE

52. The United States is unaware at this time of other attempts to obtain a warrant to search the **SUBJECT PREMISES**.

REQUEST FOR SEALING

53. This is an ongoing investigation of which the targets are unaware. It is very likely, based upon the evidence described above, that evidence of the crimes under investigation exists on computers and electronic communication accounts subject to the control of the targets. There is reason to believe, based on the above, that premature disclosure of the existence of the search warrant will result in destruction or tampering with that evidence and seriously jeopardize the success of the investigation. As described above, this investigation began in or about June 2021. PcTattletale is one of

several stalkerware websites that HSI is investigating, and many of the other websites under investigation involve targets who are believed to be overseas. For this reason, it is unrealistic to believe that the targets will soon be apprehended. The targets of this investigation have engaged in this conduct for extended periods of time. The targets, however, are sophisticated, and would likely abandon any domains or electronic infrastructure or platforms if they learned that HSI was aware of those tools. For these reasons, this Application requests that this search warrant affidavit and the accompanying application, warrant, attachments, and sealing motion be placed under seal until further order of the court.

CONCLUSION

54. Based on the foregoing, I submit there is probable cause to believe that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1030 (computer hacking), 2511 (unlawful interception of electronic communications), 2512 (sale and advertising of unlawful interceptions), and 371 (conspiracy), and that the foregoing may be located in the SUBJECT PREMISES described in Attachment A.

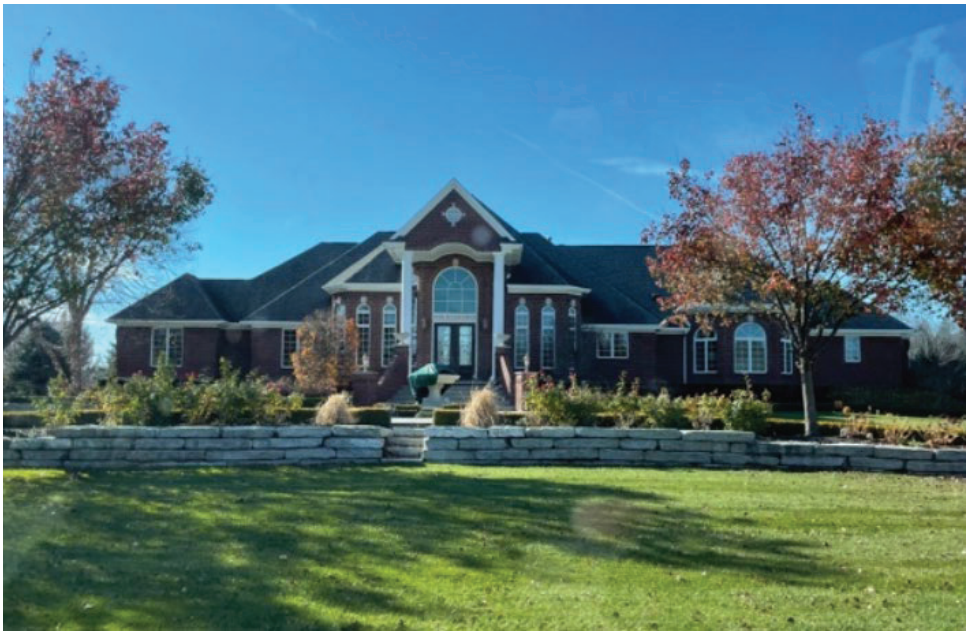
Nick Jones
Special Agent
Homeland Security Investigations

Sworn to before me and signed in my presence
And/or by reliable electronic means.

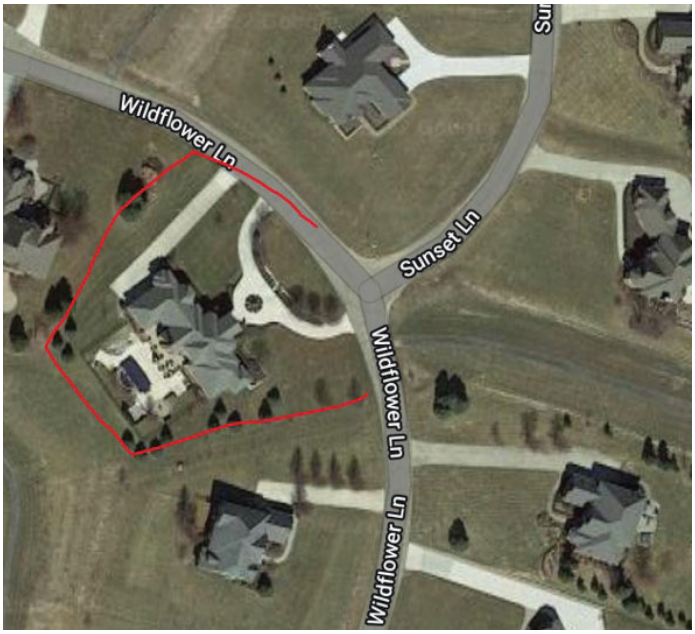
HON. ELIZABETH A. STAFFORD
U.S. MAGISTRATE JUDGE

ATTACHMENT A

The location to be searched is a stand-alone residential property located on the west side of 69951 Wildflower Lane in Bruce Township, Michigan 48065. The residence is a single-story dwelling with white columns and brick exterior with white trim.



(Image taken during recent surveillance)



(Image taken from Google Earth)

ATTACHMENT B

Authorization to search the Subject Premises described in Attachment A includes the search of computers, tablets, electronic storage devices, and cellular telephones found therein and includes deleted data, remnant data, slack space, temporary and permanent files contained on those electronic devices. The seizure and search of the any computers, tablets, electronic storage devices or cellular telephones will be conducted in accordance with the affidavit submitted in support of this warrant.

The evidence to be seized from the subject premise will be documents, receipts, packaging, records, communications, photographs, videos, images, attachments, software, hardware, social media content, screenshots, and data:

a. Tending to discuss or establish unauthorized access of phones, computers, tablets, or other electronic communication or computing devices, as well as unauthorized access of electronic communication and remote computer storage accounts and applications;

b. Tending to discuss or establish the use of hacking tools, malicious files or software, or hacking methods and techniques that enable the user to gain unauthorized access to a protected computer, cell phone, or electronic storage device or system, or distribute malicious software code that causes unauthorized damage;

c. Tending to discuss or establish the unlawful interception of electronic or oral communications;

d. Tending to discuss or establish the sale and/or advertising of unlawful interception devices;

e. Tending to identify the electronic device or software user's state of mind, including knowledge, motive, and voluntariness, regarding the crimes under investigation;

f. Tending to identify any co-conspirators involved in the activities in (a)-(d) above;

g. Tending to provide context to any communications, records, and attachments described above, such as electronic messages sent or received in temporal proximity to any relevant electronic message and any content tending to identify the user(s) of the electronic communication accounts that communicated with or about pcTattletale and the unlawful interception or unauthorized access of electronic communications; and

h. Identifying or tending to identify participants in the crimes under investigation, including the participant(s)' name(s), location(s), and date(s) of birth;

which are evidence of violations of 18 U.S.C. § 1030 (unlawful access of a computer), § 2511 (unlawful interception of electronic/oral communications), § 2512 (sale and advertising of unlawful interception devices) and § 371 (conspiracy).

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

AUSA: Robert White Telephone: (313) 226-9100
Special Agent: Nick Jones, HSI Telephone: (619) 247-8315

UNITED STATES DISTRICT COURT

for the
Eastern District of Michigan

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* 69951 Wildflower Lane, Bruce Township Michigan 48065 (More fully described in Attachment A)	Case: 2:22−mc−51755-1 Assigned To : Berg, Terrence G. Assign. Date : 11/28/2022 In re: SEALED MATTER (MAW)

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 Michigan.
(identify the person or describe the property to be searched and give its location):

See ATTACHMENT A.

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. in Violation of: 18 U.S.C.§§ 1030, 2511 Computer hacking and unlawful interception of electronic communications and 18 U.S.C.§§ 2512, 371 sale and advertising of unlawful interceptions and conspiracy to do the same.

YOU ARE COMMANDED to execute this warrant on or before 12/12/2022 *(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 the presiding United States Magistrate Judge on duty.
(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: November 28, 2022 2:51 pm

Elizabeth A. Stafford
Judge's signature

City and state: Detroit, MI

Hon. Elizabeth A. Stafford U. S. Magistrate Judge
Printed name and title

Return

Case No.:	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