99703

THE STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM CHARLESTON COUNTY
Family Court

Family Court Case No. 2022-DR-10-3072

Appellate Case No.

Justin McGee, Petitioner,

v.

Lindsay F. McGee, Respondent.

RECEIVED
AUG 30 2023
SC Court of Appeals

MOTION TO SUPPRESS EVIDENCE

This matter comes before the Court on behalf of Petitioner (the Petitioner in the pending action before the Family Court for Charleston County) by and through her undersigned counsel, who would show unto this Court, pursuant to Rule 240, SCACR, and Court News as posted and denoted as 2020-03-20-01, and S.C. Code Ann. § 17-30-110, that the relief requested here should be granted. Petitioner moves before this Court for an Order to suppress certain electronic communications between Petitioner and non-parties and between Petitioner and Respondent, based upon information and belief, her counsel of record in the pending Family Court action.

Petitioner makes this Motion on the following grounds:

1. Petitioner and Respondent are husband and wife, having been married on March 10, 2012. They are the parents of three children who are aged eight, six and three. The parties separated on or about February 21, 2021.

2. On or about September 15, 2021, Respondent gave Petitioner an iPhone 12. In exchange, Petitioner gave Respondent her iPhone 8 after she performed a "factory reset" and transferred her number 843-xxx-3367 to the iPhone 12. However, Petitioner did not remove the SIM card from the iPhone 8 before giving Respondent possession of the iPhone 8. This is significant because the SIM card gave Respondent the ability to restore the information on Petitioner's iPhone 8, thus giving Respondent access to all of Petitioner's text messages, emails, and iCloud account information.

3. As set forth in the affidavit of John Bumgarner, Petitioner is informed and believes that Respondent has been intercepting and/or reading her text and email communications since on or about September 2021, including privileged communications with Petitioners attorneys.

4. At the time of the separation, Petitioner and Respondent were members of The McGee Law Firm, LLC. Respondent was, and is, the administrator of the law firm email domain and both parties had email accounts which they utilized for personal and business. Upon information and belief it was on or about November 1, 2022 that Respondent terminated Petitioner's access to the law firm email, lindsay@mcgee-lawfirm.com.

5. On or about February 1, 2021, Petitioner moved into a home located at 664 McCutchen Circle where she has resided since that time. Respondent occasionally came to the home to visit with the children or even keep the children for Petitioner. At some point, Respondent complained that Petitioner did not have USB connections for his electronic devices and installed a power adapter with additional plugs and USB ports. Then he installed more and eventually he placed various devices throughout the house and in her garage. Attached at **Exhibit 1** is a picture of the same adapter which Respondent installed in Petitioner's garage and, upon information and belief, in other areas of her house.

6. Soon after the parties' separation, Petitioner began to have concerns that Respondent seemed to "know" about private conversations she was having with friends while Petitioner was in the privacy of her home, alone in her car, or otherwise alone and not in the presence of a third-party. Petitioner was further concerned that Respondent seemed to "know" details of pictures, text messages and/or emails between Petitioner and third parties. And that at times certain text messages and/or emails would "disappear" from her telephone" and/or her iCloud account. At some point, Petitioner would discover random password changes to her iCloud and Gmail account. When Petitioner would then go through the "forgot password" process and change her password, within hours or days, the new password would be invalid, thus requiring her to create yet another password.

7. On or about January 10, 2021, Petitioner created the email account lmcgee9310@gmail.com to ensure she had confidential communications with her then attorney, James T. McLaren. With increasing concerns that Respondent was accessing her financial information, Petitioner opened a new checking account at Bank of America on November 17, 2021 using 843-xxx-3367 as her recovery telephone number and lmcgee9310@gmail.com as her recovery email account. In September 2022, Petitioner believed that Respondent "knew" things that he should not have known and was informed and believed that Respondent was able to read her text messages. As a result, Petitioner purchased an iPhone 13 and obtained a new number (843) xxx-2168 on the same account which she used for her iPhone 8 and iPhone 12.

8. However, it was evident that Respondent continued to know about conversations Petitioner was having with third parties as evidenced by their telephone conversation and text exchange on October 2022 when he threatened her about with whom she chooses to communicate and telling her "F*** Around and Find Out", which was a phrase he often used to tell Petitioner

that if she spoke with someone that he would know about it. **[Exhibit 2]** Interestingly, John Bumgarner noted that an unknown IP address, which he suspects was Respondent, had accessed Petitioner's iCloud account on October 30, 2023.

9. Respondent reinstated Petitioner's access to her lindsay@mcgee-lawfirm.com email on May 10, 2023 after asking her to prepare some documents in a case he was working and suggesting that she use the law firm email for this purpose. **[Exhibit 3]** Petitioner logged into the account at approximately 11:14 a.m. during which time she deleted thousands of mostly junk and spam emails. Thereafter, at approximately 1:55 p.m., Respondent logged into the account, recovered the emails deleted by Petitioner, and stored them in a retention folder he named "Manage Litigation Hold." Petitioner did not log back into the lindsay@mcgee-lawfirm.com account after the May 10, 2023 login. Petitioner is informed and believes that Respondent terminated her access to this account either when he logged in on May 10, 2023 at 1:55 p.m. to create the "manage litigation hold" or in the days following the May 12, 2023 incident for which Respondent was arrested for Criminal Domestic Violence. In any event, Petitioner did not have access to the lindsay@mcgee-lawfirm.com email from November 2022 until May 10, 2023, or after May 15, 2023. **[Exhibit 4]**

10. A Temporary Hearing was held in the Family Court on June 13, 2023. Respondent's affidavit package included a copy of an email dated May 16, 2023, from Bank of America to lindsay@McGee-lawfirm.com. **[Exhibit 5]** On May 16, 2023, Petitioner no longer had access to the lindsay@mcgee-lawfirm.com email account. Respondent's counsel stated that Respondent was the system administrator for the law firm email domain and, with that authority, had legally retrieved the May 16, 2023, Bank of America from the lindsay@mcgee-lawfirm.com email account. Petitioner immediately contacted Bank of America at which time she discovered

that the lindsay@mcgee-lawfirm.com email address was added to her online banking on March 13, 2023, during the time period that Petitioner did not have access to this email account.

11. Petitioner issued subpoenas to Bank of America on June 14 and 15, 2023 to obtain the login history and other information regarding a suspected intrusion into her online account. The internal Bank of America records show that someone accessed Petitioner's bank account on Monday, March 13, 2023, at 07:20 PST (10:20 EDT) using an unidentified Apple iPhone that was connected to the AT&T cellular network. **[Exhibit 6]** At this point, Petitioner began issuing additional subpoenas to identify the individual to whom this IP address belonged. Notwithstanding, Petitioner is informed and believes that Respondent added the lindsay@mcgee-lawfirm.com email address to her online banking account because Respondent was the only person who had access to that email account at the time.

12. Thereafter, Petitioner began to delve into her suspicions that 1) Respondent was somehow accessing her text messages and emails and 2) there may also be recording devices in her home and/or automobile. On June 22, 2023, Petitioner's expert, John Bumgarner, requested access to Petitioner's Smart Home Manager Application associated with her home Wi-Fi network. This search revealed the possibility of there being covert surveillance cameras in Petitioner's home. Petitioner recalled electronic items that Respondent either gave her or placed in her home. Specifically, Petitioner identified some power adapters with additional plugs that Respondent installed in her home, as well as other potential devices. Petitioner immediately removed the plug adapters, one of which she found in the garage where Petitioner often retreats to speak on the phone with her attorney outside the presence of her children. **[Exhibit 7]**

13. On June 23, 2023, Petitioner delivered these plug adapter devices to her forensic expert Steve Abrams. Mr. Abrams disassembled the device Petitioner found in her garage and

confirmed that it contained a hidden camera. Mr. Abrams was able to extract the 16GB SD card embedded in the device and determined that the SD card contained video and audio recordings for the time period between October 9, 2022, and July 22, 2023, the date Petitioner removed this device from an outlet in her garage. The person monitoring this covert surveillance camera had allowed someone to listen to Petitioner's private conversations when the device was triggered by motion detection. There was a gap in the recordings from December 24, 2022, to April 30, 2023 as a result of someone deleting all data during that time period. The interim time gap in information unquestionably indicates that someone was accessing the device and selectively deleted information. Moreover, the deleted data included March 7, 2023 when Respondent came to Defendant's home, entered the garage, and took her golfcart.

14. Petitioner issued a subpoena to SCS Enterprises to obtain the purchase history for the covert surveillance camera discovered in her residence. SCS Enterprises' subpoena response indicates that a total of five devices identical to the device that was found in Petitioner's garage were purchased by Respondent on January 31, 2022, April 25, 2022, and July 26, 2022 and shipped to his office address 125 A Wappoo Creek Drive, Suite A, Charleston, South Carolina, 29412. **[Exhibit 8]**

15. According to the affidavit of Mr. Bumgarner, the WF-113 model of the covert surveillance camera that Respondent purchased from SCS Enterprises has the default name of GF-PH130. Petitioner's router log files indicate that there had been six different GF-PH130 named devices that have authenticated and connected to the Wi-Fi network in Petitioner's home. Mr. Bumgarner also found that all of these devices last connected to Petitioner's Wi-Fi network in July 2023 and on Saturday July 8, 2023, at approximately 21:05 EDT a device named "Justins-iPhone" was connected to Petitioner's home Wi-Fi network. **[Exhibit 9]**

16. Petitioner then issued a subpoena to PayPal through which Respondent paid for the three separate purchases from SCS Enterprises. The documents provided by PayPal reflect that Respondent purchased additional covert surveillance on January 24, 2022, from the website knowyournanny.com which sells covert surveillance cameras. **[Exhibit 10]** The devices purchased from knowyournanny.com were shipped to Respondent's office located at125 A Wappoo Creek Drive, Suite A, Charleston, South Carolina, 29412. A subpoena to Nanny Watch Services to identify the specific device purchased is outstanding. Finally, PayPal records also indicated that Respondent purchased a covert surveillance camera from Deluxe CCTV Incorporated's website on April 25, 2022, which is the same date that he purchased two covert surveillance cameras from SCS Enterprises.

17. It is significant that Respondent admitted to Petitioner that he placed the camera in her garage, but advised Petitioner that the other devices are now being kept at his office and in his home. Mr. Bumgarner notes that several of the covert surveillance cameras with the default names of GF-PH130 went offline the weekend of July 4, 2023. Upon information and belief, these devices were likely removed from Petitioner's residence prior to Friday, July 07, 2023, at 18:43 EDT, although one device came online on August 26, 2023.

18. Counsel for Petitioner respectfully submits that on its face the actions of Respondent intercepting Petitioners' Bank of America email and using that intercepted Bank of America email as evidence in court violated 18 USC §2515 which specifically prohibits the use of these recorded conversations or the use of any evidence of intercepted wire or oral communications in "... any trial, hearing, or other proceeding in or before any Court, ... of the United States, a state, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter" as well as the corresponding state statute (SC Code §17-30-65) as addressed hereinbelow.

19. Petitioner is informed and believes that Respondent committed numerous

interceptions of her electronic and aural communications in violation of the South Carolina Homeland Security Act (SC Code of Laws §17-30-10, *et seq*) and the Electronic Communications Privacy Act (18 USC §2510, *et seq.*) when he accessed the lindsay@mcgee-lawfirm.com email account to intercept, read, print and disseminate the May 16, 2023 email from Bank of America, when he intercepted and/or read her text and email communications including those with her attorneys, and when he secreted at least six Wi-Fi connected hidden cameras with microphones within petitioner's home without her knowledge and used them to monitor and record her conversations, including with her attorneys, for over a year. While both the South Carolina Homeland Security Act (§17-30-15 (4)(a)(ii)) and Title I of the Electronic Communications Privacy Act have exemptions to the interception language for systems administrators "in the normal course of [their] employment while engaged in any activity which is a necessary incident to the rendition of [their] service" (18 USC §2515(2)(a)), the conduct engaged in by Respondent, intercepting the communications of Petitioner purely to benefit his own self-interest, falls clearly outside any legitimate system administrator exemption. Petitioner is informed and believes that Respondent has already utilized one of these illegally intercepted electronic communications by providing screenshots or photographs of the May 16, 2023, Bank of America interception to the family court through his attorneys.

20. Additionally, Respondent likely also committed multiple violations of the Stored Communications Act by accessing email and electronic communications in electronic storage in Petitioner's iCloud, and Microsoft and Google email accounts. Respondent also violated the Computer Fraud and Abuse Act (18 USC §1030) by intentionally accessing a protected computer without authorization and thereby obtaining information contained in a financial record of Bank of America, a financial institution, on March 13, 2023, through May 16, 2023.

21. Petitioner respectfully submits that prior to the review, dissemination, or any use of such recordings, Petitioner may move before this Court, and hereby does move for this Court to hold an expedited hearing before an appropriate panel, to make a factual finding not only as to whether or not the intercepted communications violate the law, but also as to the other general admissibility issues relating to audio and video recordings and the information derived therefrom. SC Code of Laws §17-30-65 prohibits the introduction of any intercepted material into evidence before any court or tribunal within the state.

22. As such, Respondent's use of the material that he intercepted from the electronic and aural communications of Petitioner, and any material derivative of the intercepted material, should be suppressed, and barred from use in any litigation between the parties. Petitioner respectfully requests this honorable Court to issue an order suppressing all of the material that was intercepted by Respondent, including any and all derivative material.

23. Petitioner requested the identification of all surveillance devices and the identification of intercepted communications by Interrogatories and Request for Production served on opposing counsel on August 14, 2023, but responses are not yet due, although Counsel for Defendant made a request that Plaintiff comply with this request forthwith and deliver the requested covert cameras and electronic devices to Mr. Abrams for inspection. **[Exhibit 11]** Petitioner respectfully submits that she would be entitled to those discovery responses prior to any hearing set by this Court in this matter so as to properly prepare for the hearing.

24. Petitioner is informed and believes that since September 2021, and beginning the months prior to May 22, 2023, Respondent has monitored her actions and each and every conversation she has engaged in for conceivable nineteen months inside her home, including but not limited to countless telephone calls of which Respondent heard everything Plaintiff said to

friends, her now known paramour, and more importantly her attorneys. Petitioner is further informed and believes that Petitioner has been intercepting and/or reading her text messages since approximately September 2021, including her privileged communications with her attorneys. Petitioner is informed and believes that the genesis of virtually all evidence Respondent has compiled in this case, information that he provided to his private investigator, information he provided to his attorneys to develop their strategies and defenses, the allegations in his complaint, and his discovery requests seeking information is derived from the illegal audio/video recordings Respondent obtained from the covert surveillance cameras he placed in Petitioner's home and the text messages and emails of Petitioner that he illegally intercepted and/or read.

25. Further, Respondent engaged the services of a private investigator, John Clayton, on or about June 2022, after Respondent had been intercepting and reading Petitioner's text and email communications, after he had been accessing her Gmail account, and after May 2022 when he placed covert video/audio recording devices in Petitioner's home. Petitioner is informed and believes that the reason for engaging the private investigator and the directives including who to surveil was derived from the illegally obtained information and all evidence obtained by Mr. Clayton throughout his investigation is "fruit of the poisonous tree" and should be suppressed.

26. For these reasons and such further reasons as may appear at any hearing to be set on the matter, Petitioner hereby moves for a hearing to be held by this Court, if needed following this Court's review of this Motion and attachments, as required by S. C. Code Ann. § 17-30-110, *et seq*, and U. S. Code Ann., 18 U.S.C.A. § 2511, *et seq*, and appropriate rulings made as to the intercepted communication(s) and that in the interim, any action by the trial court below be stayed in addition to an Order requiring the immediate listing of and disclosure of all audio/video recording devices, documents and/or records concerning the interception of electronic

communications of Petitioner, plus, such other action, rulings, and other relief as may be appropriate in this matter, including but not limited to, an award of attorney's fees, costs and expenses.

27. Petitioner also moves for an order of this Court requiring the lower Court to segregate and seal the unlawfully obtained electronic communications and any evidence that has been gleaned from the use of said covert surveillance cameras and from the lindsay@mcgee-lawfirm.com email account. Petitioner believes that information should be segregated in the lower Court's file prohibiting review of said information by any Court including but not limited to Family Court, Common Pleas, General Sessions, Federal Court, either party, or the public.

28. Counsel verifies that he attempted in good faith to resolve this matter prior to filing this Motion, to no avail. Counsel also affirms to this Court that he has by copy of this Motion, notified opposing counsel, the guardian, and the Court below of this Motion.

29. This motion is further supported by the Affidavit of Petitioner **[Exhibit 12]**, Affidavit of John Bumgarner **[Exhibit 13]**, and Affidavit of Steve Abrams **[Exhibit 14]**, as well as such other evidence which becomes available prior to the hearing in this matter.

CONCLUSION

Based upon the foregoing, Petitioner respectfully requests the following relief:

30. For this Court to hold an expedited hearing before an appropriate panel, to make a factual finding not only as to whether or not the intercepted communications violate the law, but also as to the other general admissibility issues including suppressing all evidence relating to audio and video recordings, interception of text and email messages, and the information derived therefrom;

31. For a factual finding that Respondent installed covert surveillance recording devices in Petitioner's home and unlawfully obtained video and audio recordings;

32. For a factual finding that Respondent unlawfully accessed and intercepted Petitioner's text messages and emails;

33. For a factual finding that Respondent unlawfully accessed Petitioner's Bank of America personal account and intercepted Petitioner's emails from Bank of America, including the email dated May 16, 2023;

34. For a factual finding not only as to whether or not the intercepted communications violate the law, but also as to the other general admissibility issues relating to audio and video recordings and the information derived therefrom, to include any evidence from Respondent's private investigator, John Clayton;

35. For any action by the trial court below be stayed pending this court's Order.

36. For Respondent to be required to provide the immediate listing of and disclosure of all audio/video recording devices, documents and/or records concerning the interception of electronic communications of Petitioner, and to make those recording devices available, with the original SD card and link to the software to decrypt the audio, for inspection by Petitioner's expert;

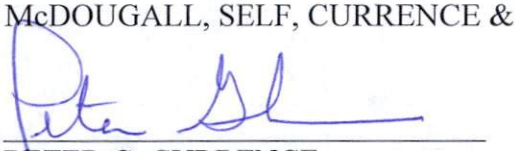
37. To determine and find that Respondent used unlawfully, obtained information to advance his case through his attorney's and exhibits;

38. For an award of attorney's fees and costs and expert fees and costs;

39. For such other and further relief as this court deems just fit and proper.

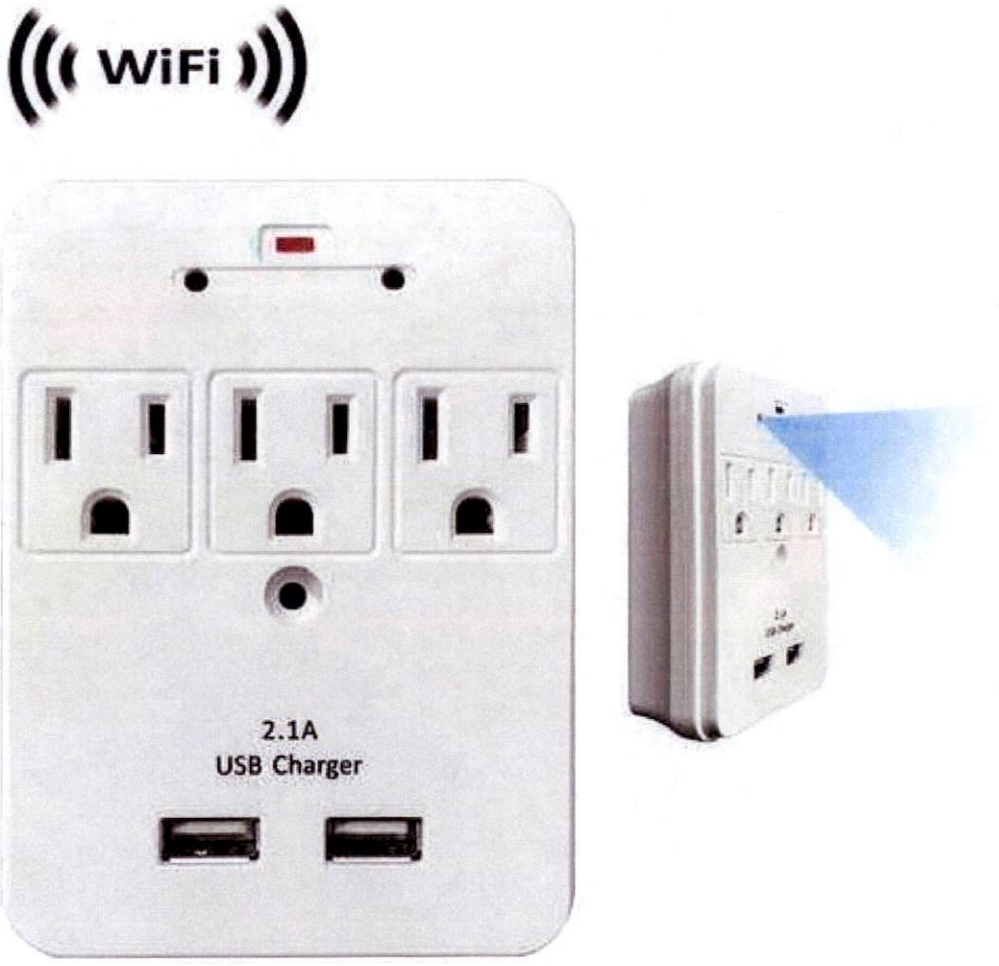
(See following page for signature block.)

McDOUGALL, SELF, CURRENCE & McLEOD, LLP



PETER G. CURRENCE
791 Greenlawn Dr. Suite 4
Columbia, South Carolina 29209
(803) 776-3130
Attorney for Petitioner

August 30, 2023


WiFi
2.1A
USB Charger

iMessage
10/30/2022 1:45:32 PM

I wish you would spend as much time figuring out how we move forward in this case as you do on social plans and scheduling visitation.

Are you still willing to work for MLF? How many billable hours per week? Compensation rate for those?

Yes I'm willing to do billable work at a rate of $250.

I'm also updating my resume and applying for jobs as a more long term solitaire.

You just called me
Irate and threatening to litigate for the next 15 years and said you didn't care who it hurts.

You are irate because I sent The popcorn fundraiser to Jay.

I can absolutely agree not to share anything kid related with him or Dan. I genuinely was just trying to raise money and get sales. I can agree not to do that in the future.

Your ugly threats are why I don't answer your calls or want to be around you.

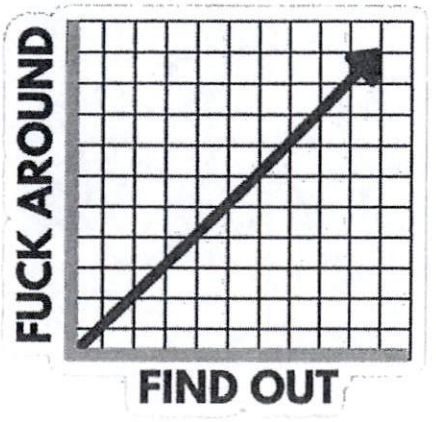
Please only call if there is a child related emergency.

I have no doubt you'll litigate about this so I'll leave it to a court to admonish me- please refrain from threatening me.

I'm not threatening though.

I said what I said and I meant it.

ONE strike rule.



10/30/22 at 2:00 p.m.

You are threatening to litigate - which hurts our kids if I "ever talk to Jay or Dan again… and you'll know."

That's absolutely absurd. You cannot control who I talk to.

You can control and have a legitimate say in who is around the kids.

You cannot control who I speak to, Justin. Once we are divorced you most certainly will have NO say in who I see - romantic or otherwise.

Replying to Justin McGee, 2022-10-30 14:08:56: « I said what I said and I meant it. »

No doubt. You already do things that hurt the kids in a thinly veiled attempt to control me.

That's the reason I left you…. And you continuing to do it now is the reason it literally makes me sick to be around you.

You can't control me or my choices either. This isn't about control, Lindsay. I've given you information. Life is about choices - you get to make one right now.

You telling me who I can
And can't speak to… that's not control?!?

I'm not telling you who you can or cannot speak to….

I'm telling you how I will respond.

Your choices have already cost you so much. Put the shovel down. It's time you definitively and finally choose your priorities and you need to do that IMMEDIATELY.

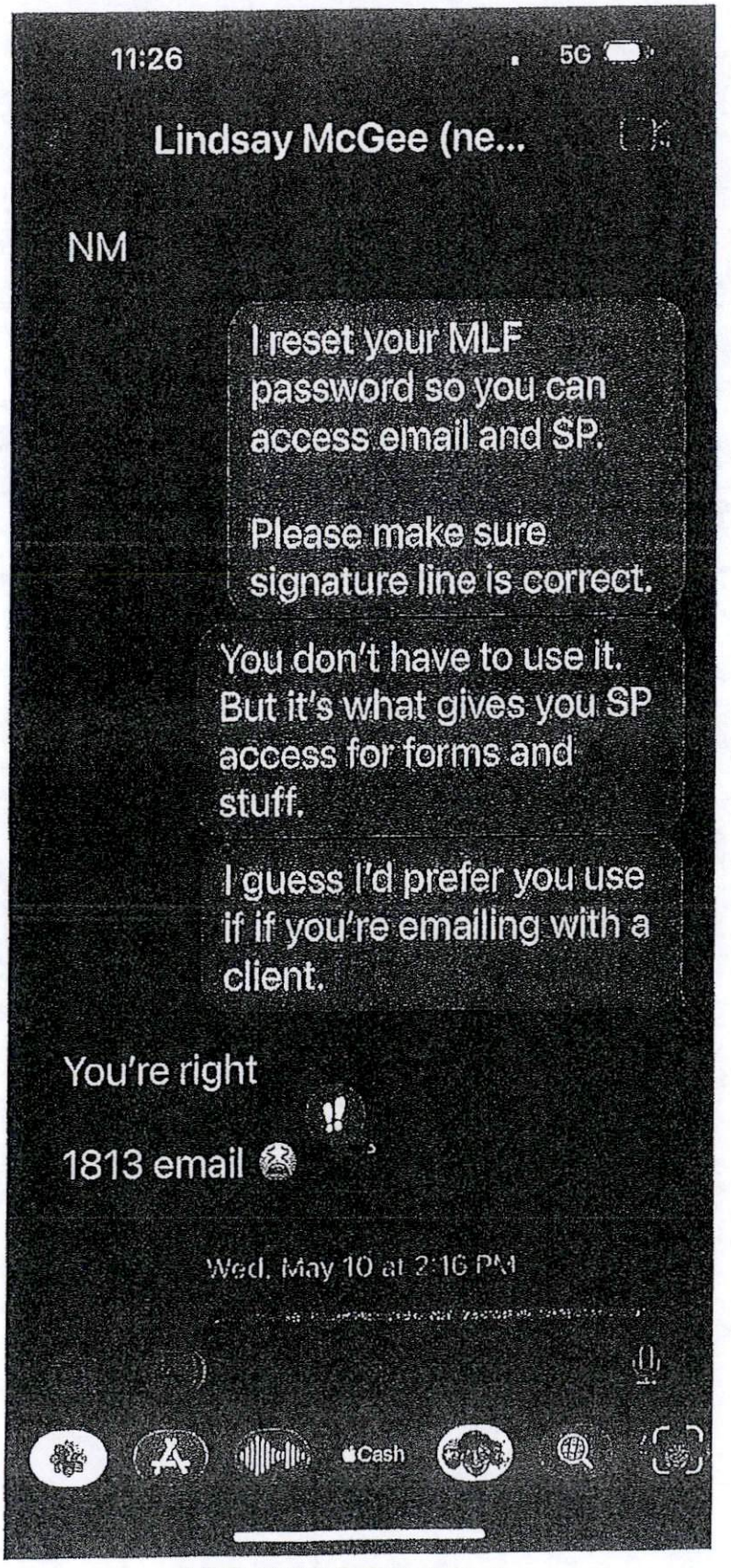
"You can't ride two mules with one ass, Sugar-bean."

Choose wisely. I'm not playing around. I'm not backing down. Don't call me begging for "all this to stop" in a month. If you can't make good decisions, I'm giving "no quarter" going forward.

Exhibit B

11:51
5G
Lindsay McGee (ne...
Wed, May 10 at 8:41 AM
Have any bandwidth for a simple ANS/CC today?
Yes
Ok. Client is
I'll have Sally send everything over.
Sally is sending everything.
Password has been reset
You've successfully reset the password for this user. We've emaili
User:
Password
lindsay@mcgee-lawfirm.com
Mug74619
Do I have to use that mine
One
Cash

Exhibit B


11:26
5G
Lindsay McGee (ne...
NM
I reset your MLF password so you can access email and SP.
Please make sure signature line is correct.
You don't have to use it. But it's what gives you SP access for forms and stuff.
I guess I'd prefer you use if if you're emailing with a client.
You're right
1813 email
Wed, May 10 at 2:16 PM
Cash

Made in USA

EXHIBIT 4

STATE OF SOUTH CAROLINA) IN THE COURT OF COMMON PLEAS
COUNTY OF CHARLESTON) THE NINTH JUDICIAL CIRCUIT
) CASE NO: 2022-DR-10-3072
Justin M. McGee,)
Plaintiff,)
vs.)
)
Lindsay McGee,)
Defendant.)
_____)

The deposition of SEAN LEONARD, GASF, EnCE, CCPA, CCO, taken before Lori Webber, Stenographic Court Reporter and Notary Public, at Andrews Mediation & Law Firm, 755 Johnnie Dodds Boulevard, Mount Pleasant, South Carolina, on Wednesday, August 2, 2023, commencing at 3:02 p.m.

A That's correct.

Q All right. Why didn't you restore any of it?

A That is not what I was asked to do.

Q Okay. So I'm assuming that you did not save a forensic copy of every deleted e-mail that would've included date, time, subject, sender information, or content; correct?

A So I did verify through images that I have there to show that everything has been put on litigation hold and archived. So I didn't do it myself, but I verified that it was done through M365.

Q When was that done?

A I don't think I have a date. I can look, though. Looking in the wrong place. Sorry; one second here. So manage litigation hold. It's turned on, and it says date hold created 5/10/2023 at 1:55 p.m.

Q Wait, date hold 5:23 p.m.?

A I'm sorry; 1:55 p.m.

Q 1:55 p.m.

A Uh-huh (witness indicated an affirmative response).

Q On May 10th?

A Yeah; May 10th, 2023, 1:55 p.m.

Q All right; what page are you looking at? Can you find it on --

A Yes; of course. Of course.

Q Count how many pages in it is.

A I organized these before I got here. I was looking at 'em --

MS. POINT: Let's do it on the one that's marked, Exhibit 1.

THE WITNESS: I have yours right here.

MR. CURRENCE: Don't mark anything on there, just tell me what it is.

MS. POINT: What page it is.

THE WITNESS: Got it.

MR. CURRENCE: Just count the pages in.

THE WITNESS: It's the second-to-the-last page of 37 pages.

BY MR. CURRENCE:

Q Okay; so there's a folder that's created that says manage litigation hold?

A It's not a folder that's created. It's basically when you click on all the mailboxes, you can see all the information about them. And so I clicked on Lindsay McGee's mailbox. And on the right-hand side, the information pops up. And in turn, you can see the information about the litigation hold.

Q Okay. And you said that was created on May the 10th?

A It says right here, yeah, May 10th, 2023, 1:55 p.m.

Q Okay. So is it a folder in her e-mail account?

A I think we'd probably say it's more like a retention. So there's usually a retention policy for things, period for things where -- you know, there's so much data within cloud, you can't keep everything; so after a certain amount of time, things just get removed.

Q So if you don't want it removed, you move it in there?

A If you don't want things removed automatically, putting an account on litigation hold solves that problem.

Q Okay; but you're not the one who put those e-mails in there, are you?

A No, the account here is Justin McGee Law Firm.

Q The administrator?

A Yeah, the hold started by Justin@mcgee-lawfirm.com.

Q Okay. All right; thank you. That clears that up.

How many e-mails were in Ms. McGee's primary inbox when she logged on at 11:14 a.m.?

A I don't know how e-mails she saw.

Q Okay; let me ask you: What time did she log in?

A So we have -- I mention it in my affidavit. Let me pull up the date.

Q Well, I guess I could've read that, couldn't I?

A It's all right.

Q Paragraph A, approximately 11:14.

A Yes.

Q On May 10th.

A Yes.

Q It was logged into.

A Yes.

Q Approximately two minutes later, a mass deletion of items was initiated and continued until approximately 12 p.m.

A Yes.

Q What time did she log off?

A I do not know.

Q Who would know that?

A I don't believe that there's any log-off information, so I pulled this from logs that show log-in information.

Q Okay. So, you didn't -- of the e-mails that were deleted, you don't know how many of those e-mails were in her primary box when she logged in at 11:14 a.m.

A That's correct.

Q Was there a way to find that out? I mean, my

Outlook has a number by it that tells me how many e-mails are in my inbox.

A Yeah.

Q And there are a lot.

A I'm sorry; can you repeat the question again?

Q Was there a way for you to determine how many e-mails were in her primary inbox when she logged in or logged on at 11:14 a.m.?

A Not from my understanding. I haven't seen anything like that.

Q Okay. You know how many e-mails were in her spam folder when she logged on at 11:14 a.m.?

A No, I do not.

Q Now, 39,000 e-mails were deleted in two minutes, but there's no -- we don't know any context about the mailbox folder location for any of those 39,000 e-mails.

A That is correct, yes.

Q So those e-mails in your affidavit -- and tell me if I'm saying this right. You state the deletions occurred from the time she logged on at 11:14 a.m. until 12 o'clock p.m., which is 46 minutes.

A Around 46 minutes, yeah.

Q Okay. And we don't know the location of those e-mails prior to them being deleted; right?

THE STENOGRAPHIC REPORTER: Brittany, do you want a copy?

MS. POINT: Yes, please.

(The deposition was concluded at 4:19 p.m.)

COURT REPORTER'S CERTIFICATE

I DO HEREBY CERTIFY THAT THE TESTIMONY CONTAINED IN SAID DEPOSITION WAS, BY ME, REDUCED TO WRITING IN THE PRESENCE OF SAID WITNESS BY MEANS OF A COMPUTERIZED TRANSCRIPTION. THE SAID DEPOSITION IS A TRUE AND ACCURATE TRANSCRIPT OF THE WHOLE OF THE TESTIMONY GIVEN BY SAID WITNESS, AS AFORESAID.

I DO FURTHER CERTIFY THAT I AM NOT CONNECTED BY BLOOD OR MARRIAGE WITH ANY OF THE PARTIES OR THEIR ATTORNEYS OR AGENTS, AND THAT I AM NOT AN EMPLOYEE OF EITHER OF THEM, NOR INTERESTED DIRECTLY OR INDIRECTLY IN THE MATTER OF CONTROVERSY EITHER AS COUNSEL, ATTORNEY, AGENT, OR OTHERWISE.

SIGNED THIS 11th DAY OF AUGUST, 2023.

_____

LORI WEBBER, NOTARY PUBLIC

My commission expires: April 7, 2027

Made in USA

You sent $500.00 to Dan

BO

Bank of America <onlinebanking@ealerts.bankofamerica.com>
To Lindsay McGee

Reply | Reply All | Forward | ...
Tue 5/16/2023 12:03 PM

If there are problems with how this message is displayed, click here to view it in a web browser.
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

You sent $500.00 to Dan

Sent from account	**ending in 4639**
To	**843-814-7131**
Your message	**Monthly friend fee**

View your balance

Confirmation	**lu16qjwb4**

If you didn't make this payment, contact us

charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	9510	1	0	0.00	SASI:SES eStatement by account	Customer selects to stop mailing paper statement by account on Sales Enablement Paper Suppression (SES) splash page.	EStatements	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	7	1	0	0.00	ALL:SignIn:Start:Validate	System validates the Online ID and Passcode that the Customer has entered at Sign-in to Online or Mobile Banking.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	12	1	0	0.00	Mobile App detection	Authenticates that the customer is using the mobile downloadable app for online banking	StartSession	11/9/2010 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	30	1	0	0.00	ALL:SignIn:Authentication: Complete	SignIn Authentication Complete and signin landing page or SASI is displayed	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	15000	1	0	0.00	MB: Start of MB Session	Indicates the start of a Mobile session (written once per session	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	15186	4	0	0.00	Targeted Ads on Accounts Page Load	On account screen page load with targeted Ad present in MDA	MarketingAd	5/28/2013 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	15400	1	0	0.00	MB: Mobile SASI banner displayed	Trigger on service call for banner presentment	MarketingAd	1/6/2015 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	15401	1	0	0.00	MB: Mobile SASI-User selection action	Selection link/button/CTA in mobile SASI	MarketingAd	1/6/2015 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.91	185593983936	IPHONE	PST	3/13/2023 12:00:00 AM	07:20:50.3200000	3/13/2023 12:00:00 AM	07:21:53.6400000	63	11190	1	0	0.00	Alerts:Payment Due Alert	Payment Due Alert setup from Paperless Splash page (new in Nov 2017) for new enrollment - 1st login	EStatements	11/8/2017 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	206.225.203.1	185577865408	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:23:40.8400000	3/13/2023 12:00:00 AM	07:23:40.8400000	0	25	1	0	0.00	Access/Data Refresh Token Validation	Access/Data Refresh Token Validation; Aggregator/Agent Data Refresh - System validates the token from aggregators/agentsTrigger: From widget for Consent		7/12/2017 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	206.225.203.7	185577241429	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:25:29.2200000	3/13/2023 12:00:00 AM	07:25:29.2200000	0	76	1	0	0.00	Aggregator:3rd Party:Tokenization	Tokenization when user first links their BofA accounts on a third party site. Bank provides a one-time AuthZ code during initial account linking. Third party exchanges AuthZ code for access token.		7/12/2017 12:00:00 AM	12/31/9999 12:00:00 AM

charlie907	charlie907	20082282031	20082282031	206.225.203.8	185589645312	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:25:31.3600000	3/13/2023 12:00:00 AM	07:25:31.3600000	0	25	1	0	0.00	Access/Data Refresh Token Validation	Access/Data Refresh Token Validation; Aggregator/Agent Data Refresh - System validates the token from aggregators/agentsTrigger: From widget for Consent		7/12/2017 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	206.225.203.9	185607473715	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:23:38.6700000	3/13/2023 12:00:00 AM	07:23:38.6700000	0	76	1	0	0.00	Aggregator:3rd Party:Tokenization	Tokenization when user first links their BofA accounts on a third party site. Bank provides a one-time AuthZ code during initial account linking. Third party exchanges AuthZ code for access token.		7/12/2017 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185578759240	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:23:01.1500000	3/13/2023 12:00:00 AM	07:23:33.1400000	32	75	1	0	0.00	Aggregator:3rd Party:Consent	User provides consent to share their account data with a third party site		7/12/2017 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185578759240	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:23:01.1500000	3/13/2023 12:00:00 AM	07:23:33.1400000	32	21120	1	0	0.00	OTAC:Load of Auth Code Page	The Auth code Request page is loaded for customer to continue the authorization process	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185578759240	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:23:01.1500000	3/13/2023 12:00:00 AM	07:23:33.1400000	32	21130	1	0	0.00	OTAC:Send Auth Code	The Auth code Request page is loaded for customer to continue authorization process due to a higher level of authentication is required to complete the current function the customer is trying to complete.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185578759240	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:23:01.1500000	3/13/2023 12:00:00 AM	07:23:33.1400000	32	21140	1	0	0.00	OTAC:Enter Authorization Code	Customer enters authorization code and selects continue button to complete authentication process.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185590767251	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:24:49.6600000	3/13/2023 12:00:00 AM	07:25:23.7200000	34	75	1	0	0.00	Aggregator:3rd Party:Consent	User provides consent to share their account data with a third party site		7/12/2017 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185590767251	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:24:49.6600000	3/13/2023 12:00:00 AM	07:25:23.7200000	34	21120	1	0	0.00	OTAC:Load of Auth Code Page	The Auth code Request page is loaded for customer to continue the authorization process	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185590767251	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:24:49.6600000	3/13/2023 12:00:00 AM	07:25:23.7200000	34	21130	1	0	0.00	OTAC:Send Auth Code	The Auth code Request page is loaded for customer to continue authorization process due to a higher level of authentication is required to complete the current function the customer is trying to complete.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM

charlie907	charlie907	20082282031	20082282031	69.47.199.158	185590767251	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:24:49.6600000	3/13/2023 12:00:00 AM	07:25:23.7200000	34	21140	1	0	0.00	OTAC:Enter Authorization Code	Customer enters authorization code and selects continue button to complete authentication process.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185597204153	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:26:36.6000000	3/13/2023 12:00:00 AM	07:28:00.0300000	83	21120	1	0	0.00	OTAC:Load of Auth Code Page	The Auth code Request page is loaded for customer to continue the authorization process	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	69.47.199.158	185597204153	NOT AVAIL	PST	3/13/2023 12:00:00 AM	07:26:36.6000000	3/13/2023 12:00:00 AM	07:28:00.0300000	83	21130	1	0	0.00	OTAC:Send Auth Code	The Auth code Request page is loaded for customer to continue authorization process due to a higher level of authentication is required to complete the current function the customer is trying to complete.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.23	185352068474	IPHONE	PST	3/9/2023 12:00:00 AM	07:48:35.6100000	3/9/2023 12:00:00 AM	07:53:17.7600000	282	5	0	1	0.00	SignIn:Preauthenticate:ID/PSWD Invalid	ISignIn:Preauthenticate:ID/PSWD Invalid	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM
charlie907	charlie907	20082282031	20082282031	166.194.154.23	185352068474	IPHONE	PST	3/9/2023 12:00:00 AM	07:48:35.6100000	3/9/2023 12:00:00 AM	07:53:17.7600000	282	7	1	0	0.00	ALL:SignIn:Start:Validate	System validates the Online ID and Passcode that the Customer has entered at Sign-in to Online or Mobile Banking.	StartSession	10/11/2009 12:00:00 AM	12/31/9999 12:00:00 AM

2.1A
USB Charger

iMessage
3/7/23, 4:54 PM

Fine. I'll pay the taxes but I'm getting my trailer and golf cart today.

The golf cart is my non-marital property - gift from a third party (Doug).

3/8/23, 10:17 AM

Well we certainly can't take the golf cart to parks anymore like we used to.

They say they hate you. You spank them. You are mean to them. You destroy their stuff. You play favorites with Amelia ... should I go on

3/23/23, 12:16 PM

Replying to you, 2023-03-23 11:54:23: « Why did you not inform them of the sale when you got the new truck coverage?!?!? WTF »

You weren't authorized to enter my garage and steal my golf cart. Even CHM remembers you gave me that for Mother's Day. Way to be a good role model for your boys.

Text message
4/2/23, 10:20 AM

Found those under the golf cart seat. Need them?

iMessage
4/2/23, 12:50 PM

I fucking hate you for stealing my golf cart

Made in USA

EXHIBIT 9

STATE OF SOUTH CAROLINA COUNTY OF CHARLESTON	)	IN THE FAMILY COURT FOR THE NINTH JUDICIAL CIRCUIT
Lindsay McGee, Plaintiff, vs. Justin M. McGee, Defendant.	)	**AFFIDAVIT OF CUSTODIAN OF RECORDS** Docket No. 2022-DR-10-3072

PERSONALLY APPEARED BEFORE ME, _____,

who first being duly sworn testifies:

1. I am Kenneth Lee. I am employed by/own SCS Enterprises, Inc, in the position of president.

2. I am the duly authorized and designated custodian of records for SCS Enterprises, Inc. and am duly authorized to certify such records.

3. I certify that the attached documents, Bates #000006-000010, which were provided to McDougall, Self, Currence & McLeod, LLP, in response to a subpoena dated July 25, 2023, are true and correct copies of the original documents from SCS Enterprises, Inc. Said records were prepared by myself on behalf of SCS Enterprises, Inc. in the ordinary course of business.

SIGNATURE Kenneth Lee

PRINT NAME Kenneth Lee

STATE OF NEW YORK
ROCKLAND COUNTY

SWORN to before me this
2 day of AUG 2023.

NOTARY PUBLIC
STATE OF NY
My Commission Expires: 3/6/27

HIRSCH ROSENZWEIG
Notary Public, State of New York
Reg. No. 01RO0002288
Qualified in Rockland County
Commission Expires 03/06/2027

Elizabeth Sheehan

From: SCS Enterprises Inc <info@spycameras.com>
Sent: Wednesday, July 26, 2023 11:27 AM
To: Elizabeth Sheehan
Subject: RE: McGee v. McGee
Attachments: packing_slip_2536_20230726T150351Z.pdf; packing_slip_2628_20230726T150625Z.pdf; packing_slip_2747_20230726T150835Z.pdf

Hi. We have found 3 records of Mr. McGee purchasing from us.

Tracking numbers and payment info:

#2536: 1Z515R660393138284 $438.00 USD was authorized on PayPal Express Checkout
#2628: 1Z515R660393511521 $438.00 USD was authorized on PayPal Express Checkout
#2747: 1Z515R660391459306 $438.00 USD was authorized on PayPal Express Checkout.

Kenneth Lee

SCS Enterprises, Inc.
http://www.wifispycameras.com
845-533-4460 :Tel
914-882-1054 :SMS

From: Elizabeth Sheehan [mailto:lizzie@mscmlaw.com]
Sent: Tuesday, July 25, 2023 16:43
To: info@spycameras.com
Cc: Pete Currence; Lori Ross
Subject: McGee v. McGee

Please see attached in regard to the above referenced matter. Should you have any questions, please do not hesitate to contact our office.

Thank you,

SCS ENTERPRISES

Order #2536
January 31, 2022

SHIP TO

Justin McGee
125 A Wappoo Creek Dr
STE A
Charleston SC 29412
United States
(843) 847-1502

BILL TO

Justin McGee
125 A Wappoo Creek Dr
STE A
Charleston SC 29412
United States

ITEMS		QUANTITY
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden In 3 AC Outlet with Dual USB Charging Port Wall Charger)) DOWN / Add Audio / 32GB WF-113D-A-32	1 of 1

Thank you for shopping with us!

SCS Enterprises
6 Fortune Way, Montebello NY 10901, United States
info@spycameras.com
wifispycameras.com

SCS ENTERPRISES

Order #2628
April 25, 2022

SHIP TO

Justin McGee
McGee Law Firm
125A Wappoo Creek Dr, STE A
STE A
Charleston SC 29412
United States
(843) 847-1502

BILL TO

Justin McGee
McGee Law Firm
125A Wappoo Creek Dr, STE A
STE A
Charleston SC 29412
United States

ITEMS	QUANTITY
WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) Straight / Add Audio / 16GB WF-113-A	1 of 1
WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) DOWN / Add Audio / 16GB WF-113D-A	1 of 1

Thank you for shopping with us!

SCS Enterprises
6 Fortune Way, Montebello NY 10901, United States
info@spycameras.com
wifispycameras.com

SCS ENTERPRISES

Order #2747
July 26, 2022

SHIP TO

Justin McGee
125A Wappoo Creek Dr
Charleston SC 29412
United States
8438471502

BILL TO

Justin McGee
125A Wappoo Creek Dr
Charleston SC 29412
United States

ITEMS		QUANTITY
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) DOWN / Add Audio / 16GB WF-113D-A	1 of 1
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) Straight / Add Audio / 16GB WF-113-A	1 of 1

Thank you for shopping with us!

SCS Enterprises
6 Fortune Way, Montebello NY 10901, United States
info@spycameras.com
wifispycameras.com

AT&T

Device | Broadband | Home Network | Voice | Firewall | Diagnostics

Status | Device List | System Information | Access Code | Remote Access | Restart Device

Device List

Home Network Devices

Clear and Rescan for Devices

MAC Address	04:7b:cb:3b:75:94
IPv4 Address / Name	192.168.1.206 / unknown047bcb3b7594
Last Activity	Mon Jul 31 09:24:36 2023
Status	on
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No

MAC Address	04:7b:cb:64:94:a5
IPv4 Address / Name	192.168.1.236 / LFM
Last Activity	Mon Jul 31 09:24:36 2023
Status	on
Allocation	dhcp
Connection Type	Ethernet LAN-4
Mesh Client	No
IPv6 Address	2600:1700:6e15:4050::49
Type	dhcp
Valid Lifetime	2592000s
Preferred Lifetime	604800s
IPv6 Address	2600:1700:6e15:4050:8026:2084:9fb2:73a5
Type	slaac
Valid Lifetime	2592000s
Preferred Lifetime	604800s
IPv6 Address	2600:1700:6e15:4050:a984:2310:ef30:dc11
Type	slaac
Valid Lifetime	2592000s
Preferred Lifetime	604800s
IPv6 Address	fe80::d107:d2bb:a739:dd58
Type	slaac
Valid Lifetime	forever
Preferred Lifetime	forever

MAC Address	08:12:a5:ce:47:6a
Name	unknown0812a5ce476a
Last Activity	Mon Jul 24 15:36:30 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No

MAC Address	0c:54:15:af:4b:00
Name	LAPTOP-4J617H8E
Last Activity	Fri Jun 16 17:12:36 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No

MAC Address	0c:8b:7d:e3:4b:0a
IPv4 Address / Name	192.168.1.252 / unknown0c8b7de34b0a
Last Activity	Mon Jul 31 09:22:54 2023
Status	on
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No

MAC Address	0c:8b:7d:f2:ff:54

Help

The device list page shows all items of the LAN Host Discovery table. Use the "Clear and Rescan for Devices" button to reset the devices table and do a fresh search for connected LAN devices.

Allocation types include static and dhcp. When the allocation type of a device has not yet been determined, it is marked pending. Devices that are powered off will continue to appear in the table, but be shown as "off" for a period of more than a day.

The Last Activity display will be blank if the WAN is down or the device cannot reach a time server.

IPv4 Address / Name	192.168.1.216 / unknown0c8b7df2ff54
Last Activity	Sun Jul 30 22:59:02 2023
Status	on
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0c:cf:89:22:5f:47
Name	unknown0ccf89225f47
Last Activity	Sat Jul 29 06:36:15 2023
Status	off
Allocation	static
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0c:cf:89:23:be:4c
Name	GF-PH130
Last Activity	Thu Jul 20 15:25:02 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0c:cf:89:50:51:f8
Name	unknown0ccf895051f8
Last Activity	Thu Jul 13 17:55:48 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0c:cf:89:a4:02:8a
Name	unknown0ccf89a4028a
Last Activity	Sun Jul 30 15:56:51 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0c:cf:89:b1:cb:93
Name	unknown0ccf89b1cb93
Last Activity	Mon Jun 12 21:46:02 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0c:ee:99:36:34:7d
Name	unknown0cee9936347d
Last Activity	Thu Jul 20 18:02:57 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	0e:0e:77:ba:8e:e3

Name	unknown0e0e77ba8ee3
Last Activity	Thu Jun 22 08:18:54 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	14:7d:da:00:47:db
Name	madisens-Air
Last Activity	Tue Jun 6 22:14:33 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	14:94:6c:24:37:60
Name	iPhone
Last Activity	Thu Jul 6 10:39:42 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	1c:1b:b5:6b:6a:5c
Name	LAPTOP-QIK7J0A1
Last Activity	Sat Jun 10 12:40:13 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	1c:45:86:05:d7:ce
Name	unknown1c458605d7ce
Last Activity	Sun Jul 16 12:43:31 2023
Status	off
Allocation	dhcp
Connection Type	Ethernet LAN-2
Mesh Client	No
MAC Address	1e:43:35:70:fa:a3
Name	Iphone-10-X
Last Activity	Fri Jul 21 22:27:53 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	2c:64:1f:b5:9f:36
IPv4 Address / Name	192.168.1.132 / unknown2c641fb59f36
Last Activity	Sun Jul 30 22:08:25 2023
Status	off
Allocation	static
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	30:7b:c9:26:1c:9c
Name	GF-PH130
Last Activity	Tue Jul 4 14:21:58 2023

Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	34:73:5a:f6:f5:bf
Name	NCGS-LEG-02
Last Activity	Tue Jul 25 17:17:34 2023
Status	off
Allocation	dhcp
Connection Type	Ethernet LAN-4
Mesh Client	No
MAC Address	38:87:d5:1e:ed:a8
Name	NCGS-LEG-02
Last Activity	Mon Jun 19 20:30:07 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	40:91:51:a6:f7:c8
IPv4 Address / Name	192.168.1.234 / Pura-F7C8
Last Activity	Mon Jul 31 09:22:53 2023
Status	on
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	42:35:a2:ae:0f:50
Name	Daniels-iPad-2
Last Activity	Sat Jun 24 14:07:21 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	42:cd:7a:d0:b1:eb
Name	unknown42cd7ad0b1eb
Last Activity	Fri Jun 23 10:11:44 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	4a:29:cd:de:db:b9
Name	unknown4a29cddedbb9
Last Activity	Thu Jun 29 10:08:39 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	4a:55:55:e3:56:45
Name	unknown4a5555e35645
Last Activity	Sat Jun 10 13:31:58 2023
Status	off
Allocation	dhcp

Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	4c:03:4f:5b:9f:fa
Name	NVTUS-7LX67M3
Last Activity	Wed Jul 12 21:06:32 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	4c:3b:df:31:db:1a
Name	XBOX
Last Activity	Tue Jul 25 23:35:46 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	54:ef:33:45:d4:b0
Name	unknown54ef3345d4b0
Last Activity	Mon Jul 10 15:53:07 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	54:f1:5f:e6:9e:3e
Name	unknown54f15fe69e3e
Last Activity	Tue Jul 11 10:54:16 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	5c:47:5e:09:2a:94
IPv4 Address / Name	192.168.1.235 / RingDoorbell-94
Last Activity	Mon Jul 31 09:20:35 2023
Status	on
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	64:ff:0a:cb:a6:91
Name	unknown64ff0acba691
Last Activity	Mon Jun 5 07:13:32 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	66:36:02:c2:46:f9
IPv4 Address / Name	192.168.1.226 / unknown663602c246f9
Last Activity	Mon Jul 31 09:22:53 2023
Status	on
Allocation	dhcp

Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	66:37:76:3d:bb:f8
Name	unknown6637763dbbf8
Last Activity	Sun Jul 30 14:16:21 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	6e:65:2f:34:14:fb
Name	unknown6e652f3414fb
Last Activity	Thu Jul 20 23:26:04 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	70:ef:00:be:a5:15
Name	iPhone
Last Activity	Sat Jul 8 21:17:33 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	7a:2b:c1:bd:9a:77
Name	iPhone
Last Activity	Sun Jul 9 11:50:39 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	80:45:dd:a6:6b:89
Name	TABLET-6NJ3LR5L
Last Activity	Fri Jul 14 05:22:36 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	80:e6:50:03:e5:12
Name	Bonnies-MBP
Last Activity	Tue Jul 18 23:27:57 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	82:99:27:da:6a:2b
Name	iPhone
Last Activity	Wed Jul 5 08:26:14 2023
Status	off
Allocation	dhcp

Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	84:a6:c8:34:0b:d4
Name	HP
Last Activity	Fri Jul 28 14:31:53 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	86:05:fd:9b:17:e0
Name	unknown8605fd9b17e0
Last Activity	Tue Jul 18 07:54:21 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	8a:97:45:e0:2b:9d
Name	Dans-iPhone
Last Activity	Mon Jun 12 14:38:41 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	8e:e1:0b:7c:eb:81
Name	Charlies-iPad
Last Activity	Mon Jun 26 13:10:07 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	92:1b:cf:0b:b0:71
Name	unknown921bcf0bb071
Last Activity	Wed Jul 26 11:48:20 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	94:db:56:fe:35:1f
Name	unknown94db56fe351f
Last Activity	Mon Jun 5 07:14:40 2023
Status	off
Allocation	pending
Connection Type	Ethernet LAN-3
Mesh Client	No
MAC Address	96:c4:b6:ca:81:a2
Name	unknown96c4b6ca81a2
Last Activity	Mon Jun 26 12:39:31 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz

	Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	a0:9f:10:32:e8:5f
Name	GF-PH130
Last Activity	Tue Jul 4 14:21:15 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	a0:9f:10:33:52:24
Name	GF-PH130
Last Activity	Fri Jul 7 18:43:54 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	a0:9f:10:3c:30:18
Name	GF-PH130
Last Activity	Tue Jul 4 14:21:58 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	a0:9f:10:6f:15:a0
Name	GF-PH130
Last Activity	Tue Jul 4 14:21:58 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	a2:a6:31:de:c2:27
Name	iPhone
Last Activity	Mon Jun 26 16:42:37 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	ae:5c:1e:ee:ed:d0
Name	unknownae5c1eeeedd0
Last Activity	Wed Jul 5 22:19:07 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	ae:62:9e:fd:f8:85
Name	unknownae629efdf885
Last Activity	Mon Jun 26 16:41:54 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz

	Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	da:e8:85:d9:9d:6a
Name	McGees-iPhone
Last Activity	Mon Jun 12 20:10:23 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	e8:a7:30:37:06:7c
Name	iPhone
Last Activity	Sat Jul 1 19:32:18 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	e8:d8:d1:bd:16:b0
Name	Lindsay-PC
Last Activity	Sat Jul 8 15:59:16 2023
Status	off
Allocation	dhcp
Connection Type	Ethernet LAN-4
Mesh Client	No
MAC Address	ea:5d:27:39:c3:17
Name	Justins-iPhone
Last Activity	Sat Jul 8 21:05:10 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	f0:6e:0b:c6:c5:9c
IPv4 Address / Name	192.168.1.146 / LFM
Last Activity	Mon Jul 31 04:08:26 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	f2:86:b4:0b:25:4a
Name	unknownf286b40b254a
Last Activity	Wed Jul 26 11:52:26 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No

© 2016-2023 AT&T Intellectual Property. All rights reserved. AT&T and Globe logo are registered trademarks of AT&T Intellectual Property.
© 2016 ARRIS Enterprises LLC. All rights reserved. ARRIS is a registered trademark of ARRIS Enterprises LLC.

	Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	ae:cd:74:a8:9f:1b
Name	unknownaecd74a89f1b
Last Activity	Thu Jul 13 12:25:53 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	ae:e5:bd:cd:9f:38
Name	unknownaee5bdcd9f38
Last Activity	Wed Jul 26 11:47:20 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	bc:09:1b:fe:80:0d
IPv4 Address / Name	192.168.1.228 / LFM
Last Activity	Sun Jul 30 22:54:42 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	bc:9e:bb:bf:a9:6d
IPv4 Address / Name	192.168.1.232 / unknownbc9ebbbfa96d
Last Activity	Mon Jul 31 09:23:32 2023
Status	on
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	bc:ce:25:f9:2a:95
Name	unknownbcce25f92a95
Last Activity	Fri Jul 21 17:53:02 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	c4:ac:59:a0:d0:8d
Name	Canona25f2c
Last Activity	Thu Jul 20 15:25:19 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 2.4 GHz Type: Home Name: ATTGRYhNQs
Mesh Client	No
MAC Address	da:26:8d:89:89:08
Name	iPhone
Last Activity	Sat Jul 1 20:20:06 2023
Status	off
Allocation	dhcp
Connection Type	Wi-Fi 5 GHz

Updated Date	USD Equivalent	Item Title	Counterparty Name	Redirect URL
01-24-2022 18:33:56	190.11	5CGRWIFI:5-Port USB WiFi Charger Cam for Home and Office:		https://knowyournanny.com/checkout
01-24-2022 18:33:56	190.11	5CGRWIFI:5-Port USB WiFi Charger Cam for Home and Office:	M.E.G.	https://knowyournanny.com/checkout
01-24-2022 18:43:25	449.94	:4K WiFi USB Power Hub Security Cam:		https://www.paypal.com/checkoutnow/error?paymentId=PAYID-MHXWHBY1W958764RN002142L
01-24-2022 18:43:25	449.94	:4K WiFi USB Power Hub Security Cam:	M.E.G.	https://www.paypal.com/checkoutnow/error?paymentId=PAYID-MHXWHBY1W958764RN002142L
01-31-2022 10:58:11	268.93	2x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access		https://wifispycameras.com/18767581/checkouts/c1a089263c4efa62b08048077cec49f7?key=72ad30f62c25cc04588224831acaab69
01-31-2022 10:58:11	268.93	2x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access	US Cam Inc.	https://wifispycameras.com/18767581/checkouts/c1a089263c4efa62b08048077cec49f7?key=72ad30f62c25cc04588224831acaab69
01-31-2022 10:58:11	268.93	2x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access	US Cam Inc.	
04-25-2022 08:37:58	463.95	BB4KWIFISOUNDBAR:Soundbar Bluetooth Audio Surround Sound Speaker With 4K UHD Wifi Camera:,:Shipping:		https://www.deluxecctv.com/checkout.php?return=paypal_standard&key=165090100733736
04-25-2022 08:37:58	463.95	BB4KWIFISOUNDBAR:Soundbar Bluetooth Audio Surround Sound Speaker With 4K UHD Wifi Camera:,:Shipping:	Deluxe CCTV Video Surveillan	https://www.deluxecctv.com/checkout.php?return=paypal_standard&key=165090100733736
04-25-2022 11:36:42	438.00	4x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access		https://wifispycameras.com/18767581/checkouts/e1c9ff2b0a224a289b641a93596b40e8?key=6caf9655dc167e73170c801f828ab26c
04-25-2022 11:36:42	438.00	4x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access	US Cam Inc.	https://wifispycameras.com/18767581/checkouts/e1c9ff2b0a224a289b641a93596b40e8?key=6caf9655dc167e73170c801f828ab26c
04-25-2022 11:36:42	438.00	4x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access	US Cam Inc.	
07-26-2022 08:15:37	438.00	4x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access		http://wifispycameras.com/checkouts/c/c80163b4628c9d53a656ea3185469d13
07-26-2022 08:15:37	438.00	4x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access	US Cam Inc.	http://wifispycameras.com/checkouts/c/c80163b4628c9d53a656ea3185469d13
07-26-2022 08:15:37	438.00	4x :WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access	US Cam Inc.	

THE STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM CHARLESTON COUNTY

Family Court

Family Court Case No. 2022-DR-10-3072

Appellate Case No.

Justin McGee, Petitioner,

v.

Lindsay F. McGee, Respondent.

AFFIDAVIT OF LINDSAY F. MCGEE

PERSONALLY APPEARED before me Lindsay F. McGee who, first being duly sworn, states as follows:

1. My name is Lindsay F. McGee, and I am thirty-eight (38) years old. Justin McGee and I were married on March 10, 2012. We have three children who are aged eight, six and three. Justin and I separated on or about February 21, 2021.
2. I started making plans to separate from Justin in early January 2021. I found a rental home located at 664 McCutchen Circle on James Island but did not initially inform Justin of my intent to separate. I planned to set up the rental home and make it suitable for my children prior to informing Justin of my desire to leave our marriage. Only a few days after signing the lease, I observed Justin slowly driving by the residence.
3. I immediately called Justin and inquired about what he was doing. Justin said he was just driving around. I confronted Justin about seeing him drive by the home. Justin

admitted he was looking for me, but he claimed that it was purely coincidental that he found me and ended up driving by the residence. The rental home is in a cul-de-sac, and it would have been extremely unlikely that Justin would have driven by the residence without knowing my exact location.

4. When I informed Justin of my desire to leave our marriage and separate, he offered do anything to save our marriage. When I informed Justin there was no chance of reconciliation, he said it would be in the best interests of our children for us to work out an agreement.

5. Justin and I are both practicing family law attorneys and partners of McGee Law Firm, LLC. I initially believed that we could draft an agreement without the need to retain our own attorneys.

6. On or about September 15, 2021, Justin expressed that my iPhone 8 did not have a very good camera, and that I should have a newer iPhone if I was going to take pictures of our children during my parenting time. Justin presented me with an iPhone 12 pro max and asked that I take pictures of our children so that Justin could have as many high-quality photos of the children as possible. In return Justin asked that I give him my old iPhone 8 for use as a backup phone for the law firm. This request did not seem unusual because we always had an older iPhone that phone calls were forwarded to when our phone system went down. I initiated a complete factory reset of the iPhone 8 and made sure my data was deleted from the phone. I did not remove the internal SIM card prior to delivering the phone to Justin.

7. I sought employment outside of McGee Law Firm and was hired as corporate counsel for a pharmaceutical clinical research organization. The position was primarily a remote position, and I used my cellphone to communicate with all other members of

the executive team. Justin began to make off-hand comments about the amount of communication I was having with male members of the executive team. I dismissed these comments because Justin had always been a jealous person – any communication I had with another male was deemed inappropriate.

8. In the Spring of 2022, more than a year after my separation from Justin, I texted with a former sorority sister about her annual family vacation to Kiawah Island. My friend said she knew of a single bachelor in Charleston and sent me a text message with a photo to see if I was interested. I expressed interest in meeting the individual, but no concrete plans were ever made.
9. I made plans to see my friend over Father's Day weekend while she was staying on Kiawah Island. Justin voiced his objections and demanded that he be invited. I informed Justin he was not invited and was no longer welcome at events with my friends or family. On Saturday, June 18, 2022, I happened to be in the front of the residence when I observed Justin slowly driving by my friend's rental house.
10. Several days later I confronted Justin about what I observed, and he claimed it was a coincidence. Justin then accused me of meeting another male which I denied. Justin provided me with details of my whereabouts the previous weekend. I believed Justin had somehow gained access to my iCloud account and was able to view my text messages because he knew information that was limited to text message communication with my friend. Justin also knew of and immediately confronted me about downloading the Hinge dating application to my cellphone.
11. On September 2, 2022, I made plans with a friend to go out and celebrate my birthday. I spoke inside my home with this friend about my desire to go to a particular establishment because there was an employee whom I found attractive. I sent a text

message to my friend confirming the location of where we would meet. Justin was able to direct his private investigator to the location where I planned to meet my friend to celebrate my birthday. I understand Justin initially hired a private investigator in June 2022, but the weekend of September 3, 2022, was the first instance of direct surveillance by the investigator.

12. I committed adultery with Dan Fowler (D.F.) on September 4, 2022, and was almost immediately confronted by Justin. Initially my contact with D.F. was sporadic, but we grew closer and began to see each other more often. I continued to see D.F. and after each interaction, Justin would aggressively confront me about my whereabouts and communication with D.F. I began to see a pattern – D.F. would send me a sexually suggestive text message, and the following day Justin would rage and threaten to withhold our children to punish me for interacting with D.F.

13. As our communications became more hostile, Justin began to make threats about what he would do if I chose to litigate our case. Justin threatened that he could make my text messages say anything he wanted. Justin was able to tell me very specific things I searched on Google when I accused him of unauthorized entry into my iCloud account. Justin seemed to know everything I did using my phone – who I texted, what I searched and where I was located at any given time.

14. On October 30, 2022, Justin called me irate because I emailed a boy scout fundraiser to a male friend (J.F.). During our conversation, Justin demanded I never speak to D.F or J.F. ever again. Justin said he would know if I ever spoke with them again and texted me the date and time to mark the last point I was allowed to communicate with D.F. and J.F. Justin texted me a meme with the phrase, "Fuck around and find out." Justin

threatened that if I ever spoke to D.F. or J.F. again he would litigate our case for the next 15 years or until our youngest child turned 18. **[Exhibit 1]**

15. On February 28, 2023, I communicated with D.F. about staying at my house overnight, and on the following morning of March 1, 2023, Justin entered my home through an unlocked back door and said he needed extra clothes for one of my children. Justin was irate and questioned me about D.F.'s whereabouts in front of my children.

16. The following week on March 7, 2023, I made plans for lunch with D.F. following a job interview. Justin sent me a text message while I was with D.F. informing me that he was taking my golf cart from my garage without my permission and over my objections. I believe Justin knew where I was and that I would be unable to get home to prevent him from taking the golf cart.

17. My interactions and communications with Justin continued to escalate. On May 12, 2023, Justin came to my home heavily intoxicated and assaulted me in front of our children. Justin was arrested and charged with CDV I and aggravated burglary. He is currently on interim suspension by Order of the Supreme Court. The burglary charge has been dismissed and the CDV I was reduced. However, the Solicitor's office was not aware of Justin's obsessive stalking me with GPS trackers, his use of covert video and audio cameras in my house, or the evidence that he has been accessing my emails and text messages.

18. A temporary hearing in our case was scheduled for June 13, 2023. I prepared several drafts of an affidavit addressing numerous problems that occurred throughout my marriage to Justin and events that occurred following our separation. While not all issues made it to the final draft, Justin's affidavit seemed to address every allegation that I touched on in different drafts of my affidavit. Justin's affidavit also addressed

allegations that were made by my witnesses regarding his use of marijuana. My witnesses emailed me drafts of their affidavits prior to the temporary hearing. I believe Justin was able to access my email account and review my witness affidavits allowing him to proactively address the allegations contained therein.

19. Justin's affidavit included an email dated May 16, 2023, from Bank of America to my Lindsay@mcgee-lawfirm.com email address giving notice of a Zelle transfer. I immediately called Bank of America and learned that this email address was added to my account on March 13, 2023. I did not do this. After sending out numerous subpoenas, and my experts interpreting the data we received, there is no question that Justin added the Lindsay@mcgee-lawfirm.com address to my online account. He is the only person who had access to that account, he was clearly reading the emails, and he is the only person who would gain anything by doing this. He also has my old iPhone 8 with the recovery phone number for my Bank of America account.

20. I learned in July 2023 that Justin placed several hidden cameras inside my home with remote audio and video capabilities. I located one of the devices and my forensic expert was able to determine that video from the month of March 2022 was deleted from an internal SIM card inside the camera. I understand that Justin had the ability to delete these files from a remote location, and it is my belief that Justin wanted to delete evidence of his unauthorized entry into my home on March 1 and 7, 2023.

21. There is without question that Justin had six, if not thirteen, recording devices in my home. The data we have obtained, and the circumstances reflect that Justin intruded into my Bank of America account and was intercepting emails. Based upon all the data described in John Bumgarner's affidavit, Justin has been intercepting and/or reading every one of my text and emails with my attorneys. Based upon all the data described

John Bumgarner's affidavit, including data reflecting that the same IP address that logged into my Bank of America account also logged into my Gmail account, it is very evident that Justin has been accessing my Gmail account.

22. After two years or intercepting my electronic communications and more than one year of watching and listening to everything that I said and did in the privacy of my own home, I cannot imagine that there is any evidence Justin currently has that was not either illegally obtained or derived as a result of the illegally obtained evidence.

23. I am asking for the relief requested in my motion, to specifically include an Order requiring Justin to pay my attorney's and expert fees, which are appropriately, but shockingly high. I have incurred an estimated $50,000 alone in expert fees and I respectfully submit that their extraordinary expertise was necessary to discover the degree of Justin's cyber warfare.

24. I am over the age of twenty-one (21) years and competent to testify to the matters stated herein. I have read the foregoing paragraphs, all matters stated there are correct and true and are based upon my own personal knowledge and belief, except those alleged on information and belief and as to those, I believe them to be true and accurate.

LINDSAY MCGEE

Sworn and subscribed before me
this 29th day of August, 2023.

NOTARY PUBLIC FOR SOUTH CAROLINA
My Commission Expires: 04127/2031

ALLISON HINNANT NOTARY PUBLIC SOUTH CAROLINA My Comm. Exp. April 27 2031

THE STATE OF SOUTH CAROLINA

In The Court of Appeals

APPEAL FROM CHARLESTON COUNTY

Family Court

Family Court Case No. 2022-DR-10-3072

Lindsay F. McGee Petitioner

v.

Justin McGee Respondent

AFFIDAVIT OF JOHN BUMGARNER

PERSONALLY APPEARED BEFORE ME, the undersigned, who, being duly sworn, deposes and states the following:

Background

1. My name is John Bumgarner. I am a retired member of the US Armed Forces, where I specialized in intelligence and special operations. I have performed work for the Central Intelligence Agency, Defense Intelligence Agency, National Security Agency and the United States Special Operations Command. My current fields of concentration are cybersecurity and network forensics. I have a Master Degree in Information Systems and one in Security Management. I have been a Certified Information Systems Security Professional (CISSP) for 24 years and a Systems Security Certified Practitioner (SSCP) for 22 years. I have assisted in the exam development for both of these internationally recognized cybersecurity certifications. I was one of the first GIAC Incident Handler (GCIH) certified worldwide. I have published dozens of articles on cybersecurity and cyberwar. And I have lectured on these topics at the Naval Postgraduate School, King's College London, Queen's University Belfast and other institutions. Some of my research in my fields of expertise have been used by multiple organizations, including the Atlantic Council, Department of Defense and the North Atlantic Treaty Organization (NATO). This research has also been used in hundreds of articles, books and studies that have been published. Additionally, I have consulted on various projects with the Federal Bureau of Investigation, the United States Secret Service and the Department of Homeland Security. I am currently based out of an office

in Asheville, North Carolina. My full credentials are included in my CV which is appended to this affidavit.

2. On Monday, July 10, 2023 the law firm McDougall Self Currence McLeod headquartered in Columbia, South Carolina retained my consulting services to investigate alleged cyber intrusions into various accounts owned by their client Lindsay McGee. My role has now become that of a testifying expert.

3. My investigation into the alleged cyber intrusions required a detailed analysis of multiple pieces of technical data. This affidavit is designed to provide an in-depth explanation of the data that was available for analysis. This affidavit also contains my conclusions and opinions based on the evidence.

Investigation

Bank of America Account Intrusion

4. Steve Abrams of Abrams Cyber Law & Forensics based in Mount Pleasant South Carolina, also working forensics on this case for attorney Peter Currence, provided me with the IP logs for Lindsay McGee's Bank of America account, which were obtained through a subpoena. I was also provided records for Lindsay McGee's iCloud account with the Apple IDs of lindsayforeback@redacted and lmcgee9310@redacted. These iCloud records were also obtained via a subpoena.

5. The Bank of America IP logs contained IP addresses, device types and transaction history for Ms. McGee's bank account. The internal Bank of America records indicate that there were two separate intrusions into Ms. McGee's bank account in the month of March, 2023.

6. The first intrusion, which was previously unknown, occurred on Wednesday, March 01, 2023 at 11:36:50 PST (14:36:50 EST) using an unidentified mobile device. This device was connected to the AT&T cellular network and was assigned the IP address 166.205.218.83. According to additional subpoena data, this IP address was leased by Wireless Data Service Provider Corporation (WDSPCo) to AT&T Mobility, which is also known as AT&T Wireless. The unknown subject of this session requested consent to link Ms. McGee's bank account to a third-party site, which was Envestnet by Yodlee, Inc. The bank's records indicate that the unknown subject received an authorization code (one-time AuthZ code) to complete this linking. This AuthZ code was transmitted by the bank to an unidentified telephone number via a text message (SMS - Short Message Service). This authorization code is part of a two-factor authentication (2FA)

security system used by Bank of America to limit fraudulent activities. The Bank of America records indicate that this code was required due to the *"higher level of authentication required to complete the current function the customer was trying to perform."* I can theorize that this authorization code was sent to an unidentified mobile device that was being used to access Ms. McGee's Bank of America account. The Bank of America records reflect that the telephone contact number for this account is 843-xxx-3367. Additional information from Bank of America should confirm where the bank sent this authorization code.

7. A second session was simultaneously connected with the session identified in Item 6 of this affidavit. This session was started on Wednesday, March 01, 2023 at 11:37:28 PST (14:37:28 EST) using an unidentified device. The unknown subject initiated an Envestnet session to Ms. McGee's bank account. This session was likely executed by an unknown subject logged into Envestnet's online portal using a web browser. The Bank of America records indicate that this session originated from the IP Address 216.34.60.11. A search of the American Registry for Internet Numbers (ARIN) shows that this IP address is assigned to the business entity Yodlee, Inc. According to the internal records provided by Bank of America, these accounts had never been linked prior to Wednesday, March 01, 2023 at approximately 11:37:28 PST (14:37:28 EST). Additional information from Yodlee, Inc should confirm the Envestnet account and subscriber information related to the unknown subject that linked the accounts. The last transaction timestamp associated with these initial suspicious sessions was 12:07:44 PST (15:07:44 EST).

8. The second intrusion, which originally prompted my investigation occurred on Monday, March 13, 2023. The bank's records show that someone accessed Lindsay McGee's bank account on Monday, March 13, 2023 at 07:20 PST (10:20 EDT) using an unidentified Apple iPhone. This device was connected to the AT&T cellular network and was assigned the IP address 166.194.154.91. According to additional subpoena data, this IP address was leased by Wireless Data Service Provider Corporation (WDSPCo) to AT&T Mobility, which is also known as AT&T Wireless. According to the bank's internal records the unknown subject that accessed Ms. McGee's bank account with the unidentified Apple iPhone used valid credentials (Online ID and Passcode).

9. Simultaneously someone initiated an Intuit QuickBooks session to Ms. McGee's bank account. This session was likely executed by an unknown subject logged into Quickbooks' online portal using a web browser. The Bank of America records indicate that this session originated from the IP Address 206.225.202.1. A search of the American Registry for Internet Numbers (ARIN) shows that this IP address is assigned to the business entity Intuit Inc. The Bank of America records show that the unknown subject that accessed Ms. McGee's bank account from QuickBooks also used valid

credentials. These valid credentials allowed the unknown subject to link an unidentified QuickBooks account to Lindsay McGee's Bank of America account. According to the internal records provided by Bank of America, these accounts had never been linked prior to Friday, March 13, 2023 at approximately 07:25 PST (10:25 EDT).

10. A third session was also initiated concurrently with the previous two sessions. This session utilized the IP address 69.47.199.158. A search of the American Registry for Internet Numbers (ARIN) shows that this IP address is assigned to the business entity Wide Open West (WOW!). WOW! is one of the nation's leading broadband providers. The company provides high-speed Internet services, TV, phone, business data, voice and cloud services. The records that were provided by Bank of America have no additional information about the device that initiated this connection. According to the bank's internal records the unknown subject also used valid credentials for this session. A geolocation search for this WOW! A geographical location search shows that this IP address is located in the area of Charleston, South Carolina and is assigned to an unidentified broadband subscriber. Additional information is required from WOW! to confirm who the registered user of this IP address was on the date and time in question.

11. This third connection was most likely performed from a computer (laptop or desktop) using a web browser. According to the Bank of America records the unknown user of this session requested consent to link Ms. McGee's bank account to a third-party site, which was the Intuit Quickbooks application. The records indicate that the unknown subject entered an authorization code (one-time AuthZ code) to complete this linking. This AuthZ code was transmitted by the bank to an unidentified telephone number via a text message (SMS - Short Message Service). This authorization code is part of a two-factor authentication (2FA) security system used by Bank of America to limit fraudulent activities. The Bank of America records indicate that this code was required due to the *"higher level of authentication required to complete the current function the customer was trying to perform."* I can theorize that this authorization code was sent to the Apple iPhone that was used to access Ms. McGee's Bank of America account. The Bank of America records reflect that the telephone contact number for this account is 843-xxx-3367, which was the number associated with Ms. McGee's old iPhone 8. Additional information from Bank of America should confirm where the bank sent this authorization code. The last transaction timestamp associated with these suspicious sessions currently being investigated was 07:28 PST (10:28 EDT).

Google IP Logs for Ms. McGee's Gmail Accounts

12. On Friday, July 28, 2023, attorney Currence transmitted a subpoena to Google to obtain login information related to Lindsay McGee's Gmail accounts, which are

lindsayforeback@redacted and lmcgee9310@redacted. On Tuesday, August 22, 2023 Google responded to this subpoena with login history from the period of Friday, November 11, 2022 to Saturday, July 22, 2023.

13. Google's IP Logs indicate that IP address 166.194.154.91 connected to the AT&T cellular network logged into Ms. McGee's Gmail account lmcgee9310@redacted on Sunday, March 12, 2023 at 19:46:36 GMT (14:46:36 EDT). The unknown subject of this intrusion was using an iPhone with an operation system that was released by Apple in November 2022. That operating system was iOS 16.1.1. Ms. McGee's current iPhones are ruled out since her iPhone 12 has iOS 16.5.1 installed and her iPhone 13 has iOS 16.6 installed. This outdated operating system is an indication that the unidentified Apple iPhone used to access Ms. McGee Gmail account *has not been* updated since at least November 2022 and is most likely an older model of iPhone.

14. The IP address 166.194.154.91 identified in Item 13 of this affidavit is the same IP address that was used in the Bank of America intrusion mentioned in Item 8 of this affidavit. That intrusion occurred on Monday, March 13, 2023 at 07:20 PST (10:20 EDT). The unknown subject in both of these intrusions used an unidentified Apple iPhone.

15. The time period between the Gmail intrusion on Sunday, March 12, 2023 and the Bank of America intrusion on Monday, March 13, 2023 was approximately 20 hours. Based on this evidence the unknown subject was mostly likely stationary and did not switch cellular towers.

16. Google's IP Logs indicates that IP address 69.47.199.158 accessed Ms. McGee Gmail account on March 22, 2022 at 17:06:00 GMT (12:00 EDT). This IP Address is assigned to the business entity Wide Open West (WOW!). A geographical location search shows that this IP address is located in the area of Charleston, South Carolina and is assigned to an unidentified broadband subscriber. Additional information has been subpoenaed from WOW! to confirm who the registered user of this IP address was on the date and time in question.

17. The IP address 69.47.199.158 identified in Item 16 of this affidavit is the same IP address that was used in the Bank of America intrusion mentioned in Item 10 of this affidavit. That intrusion occurred on Monday, March 13, 2023. The unknown subject in both of these intrusions used an unidentified system running Microsoft Windows 10 with a 64-bit architecture. The browser for both of these sessions was Google Chrome 111.0.0.0.

18. The is electronic evidence indicates that the unidentified Apple iPhone mentioned in Item 13 of this affidavit accessed Ms. McGee's Gmail account lmcgee9310@redacted multiple times between November 2022 and June 2023. This unrestricted access provided the unknown subject with the capabilities to read, write, delete and forward emails in Ms. McGee's Gmail account. This email account was used by Ms. McGee to communicate with her attorney Peter Currence. Their attorney client privilege communications started in November 2022, so the evidence indicates that any conversations were intercepted and/or read by the unknown subject that compromised Ms. McGee's Gmail account lmcgee9310@redacted.

19. On Tuesday, June 13, 2023, there was a hearing on the above captioned case. On Monday, June 12, 2023, the day prior to the hearing Justin McGee had his affidavit notarized (time unknown). The electronic evidence indicates that the unidentified Apple iPhone mentioned in Item 13 of this affidavit was continually accessing Ms. McGee's Gmail account lmcgee9310@redacted prior to the court hearing. The unknown subject maintained their access to Ms. McGee's Gmail account for the entire month of May 2023 until Monday, June 12, 2023 at 14:56:34 GMT (09:56:34 EDT), which correlates with the date Justin McGee had his affidavit notarized (time unknown).

20. The unknown subject that was accessing Ms. McGee's Gmail account logged back into this account on Thursday, June 15, 2023 at 20:43:36 GMT (15:43:36 EDT). This unknown subject maintained their access to Ms. McGee's Gmail account until Thursday, June 22, 2023 at 00:15:35 GMT (20:15:35 EDT, which is Wednesday, June 21, 2023). This ending date is significant, because at 17:20 EDT on this date Lindsay McGee's attorney Peter Currence sent an email to Justin McGee's attorneys Jerry Theos and Marie Louise Ramsdale with approximately nine "Notice of Taking Deposition" that were going to be served on Thursday, June 22, 2023. Approximately 5 hours after this email was transmitted to Mr. McGee's attorneys the unknown subject stopped accessing Ms. McGee's Gmail account. Google's IP Logs show that the unknown subject stopped accessing Ms. McGee's Gmail account on Wednesday, June 21, 2023 at 20:15:35 EDT and has not resumed their access since attorney Currence's email was sent to Mr. McGee's attorneys.

<u>AT&T records for Ms. McGee's account</u>

21. On Thursday, August 03, 2023, attorney Currence transmitted a subpoena to AT&T to obtain wireless subscriber information and history related to Lindsay McGee's telephone number, which are 843.xxx.2168 and 843.xxx.3367. On Wednesday, August 23, 2023 AT&T responded to this subpoena with wireless subscriber information,

including account notes for the period of Tuesday, February 2, 2021 to Wednesday, December 07, 2022.

22. The AT&T records show that Ms. McGee added a new phone to her account on Monday, September 13, 2021. This phone was an iPhone 12 Pro Max with the serial number G0NG50GY0D46. According to Ms. McGee the iPhone 12 was a gift from her estranged husband Justin McGee. Mr. McGee asked Ms. McGee to give him her iPhone 8, which was the device being replaced by the iPhone 12 Pro Max. The iPhone 8 and iPhone 12 Pro Max telephone number was 843.xxx.3367.

23. The AT&T records show that Ms. McGee purchased an iPhone 13 with the serial number RXP447XF9P on Wednesday, September 07, 2022 with the number 843.xxx.2168 assigned by AT&T. Ms. McGee stated that she purchased this iPhone 13, because she suspected that her estranged husband Justin McGee was potentially reading her emails and text messages being sent from her iPhone 12.

24. Prior to giving her estranged husband Justin McGee the iPhone 8, Ms. McGee performed a "factory reset" of the device. A "factory reset" is designed to delete all installed applications and content stored on the device. Ms. McGee did not remove the Subscriber Identity Module (SIM) card from this iPhone 8. This SIM Card was linked to the number 843.xxx.3367.

25. The iPhone 12 Pro Max was linked to the iCloud account with the Apple ID lindsayforeback@redacted. This Apple ID was also linked to the iPhone 8 in Justin McGee's possession. Ms. McGee has stated in our conversations that she did not change her iCloud account password after providing the iPhone 8 to her estranged husband Justin McGee.

26. Ms. McGee's iCloud account contained a complete backup of her iPhone 8. Anyone knowing Ms. McGee's Apple ID lindsayforeback@redacted and the associated password for the account could install this backup on another iPhone, including the iPhone 8 that Justin McGee's was in possession of in September, 2021. Anyone installing this backup on an iPhone would have complete access to all information contained in the backup, which can include photos, videos, calendar entries, contacts, emails, documents and text messages.

27. An unidentified Apple iPhone was used in the Google Gmail intrusion identified in Item 13 of this affidavit and the Bank of America intrusions mentioned in Item 6 and 8 of this affidavit. This unidentified Apple iPhone used Bank of America's mobile banking application during the banking intrusion of Ms. McGee's account on Friday, March 13,

2023. Ms. McGee's iCloud backup contained this mobile banking application with the embedded credentials, which would allow someone to gain access to her bank account.

28. Bank of America records indicated that the contact email for Lindsay McGee's account is lmcgee9310@redacted, which is the Gmail account identified in Item 13 of this affidavit as being compromised. As stated above, the bank's records indicated that the contact number on file is 843.xxx.3367. This number is linked to the iPhone 12 Pro Max with the serial number G0NG50GY0D46 in Ms. McGee possession and to the iPhone 8 that she provided to her estranged husband Justin McGee in September, 2021. There is currently an outstanding subpoena seeking information on the authorization code (one-time AuthZ code) transmitted by Bank of America to a phone number during the banking intrusion mentioned in Item 6 through item 11 of this affidavit. Bank of America records indicate that this authorization code would have been transmitted to the number on file, which is 843.xxx.3367.

29. Current evidence strongly suggests that the iPhone 8 linked to the number 843.xxx.3367 was used in the banking intrusion mentioned in Item 6 through item 11 of this affidavit. The evidence also strongly suggests that the iPhone 8 was fully recovered from a backup contained in Ms. McGee's iCloud account. On Thursday, August 24, 2023 Ms. McGee's attorney Peter Currence sent an "Preservation Request" email to Justin McGee attorneys Jerry Theos and Marie Louise Ramsdale for the iPhone 8.

30. This "Preservation Request" also mentioned the purchase and installation of the software application iMazing. This software was purchased by Justin McGee on Saturday, September 11, 2022 using a PayPal transaction linked to an American Express card. iMazing is an application that can be used to create backups of Apple iPhones and iPads. These backups can be created from a device that is physically connected to a computer or stored in an iCloud account. My working professional theory is that Justin McGee used iMazing to make backups of the iPhone 8 linked to Ms. McGee's iCloud account. The iMazing purchase coincides with Ms. McGee's purchase of an iPhone 13, which is also linked to Ms. McGee's iCloud account. A detailed forensic analysis of the computer system that the iMazing application is installed on is required to determine how Mr. McGee used the application.

Apple iCloud records for Ms. McGee's account

31. The subpoena data provided by Apple on Lindsay McGee's primary iCloud account indicates that there was a substantial amount of activity on Sunday October 30, 2022. This device was connected to the AT&T cellular network and was assigned the IP

address 166.205.218.29. According to additional subpoena data, this IP address was leased by Wireless Data Service Provider Corporation (WDSPCo) to AT&T Mobility, which is also known as AT&T Wireless. Apple's records show that Lindsay McGee changed her Apple ID linked to her iCloud account on or about November 3, 2022. She also changed her password multiple times after the October 30, 2022 event. Preliminary data suggests that an unknown subject potentially had access to Lindsay McGee's iCloud account. This access would give the unknown subject complete access to all photographs, emails, text messages and documents stored in Lindsay McGee's iCloud account. There is circumstantial evidence that Justin McGee had access to her iCloud accounts.

Router Logs from Ms. McGee's Residence

32. Lindsay McGee believed that her estranged husband Justin McGee might have installed listening devices in her residence. On Thursday, June 20, 2023, Ms. McGee gave Peter Currence verbal authorization for me to access her AT&T Smart Home Manager. Subsequently Peter Currence gave me written permission at 17:14 EDT to access her Smart Home Manager. This application is used to manage and monitor access to the Wi-Fi network within her private residence.

33. On Friday, June 21, 2023 at 17:17 EDT I was provided with the login credentials to access the Smart Home Manager application associated with her home Wi-Fi network. A preliminary review of the Smart Home Manager, which manages an Arris BGW210-700 (DSL modem) indicated that there were 8 connected Wi-Fi capability devices in her residence. These devices included multiple televisions, a personal computer, a Nintendo Switch and other Internet of Things (IoT) devices. On Saturday, June 22, 2023 at approximately 09:00 EDT, I accessed her Smart Home Manager to conduct a detailed review of the historical devices that had previously connected to her Wi-Fi network using valid credentials, which are the Service Set Identifier (SSID) and the associated password. These credentials must be entered by any electronic devices to connect to the Wi-Fi network in Lindsay McGee's private residence.

34. The detailed review of the historical devices connected to her Wi-Fi network indicated that six unique devices named GF-PH130 had been previously connected. GF-PH130 is the nomenclature for a wireless pinhole camera developed by the Chinese company Shenzhen Goodflys Technology Corporation Limited. The company is based in Shenzhen, China. I immediately notified her attorney Peter Currence about the possibility of there being covert surveillance cameras in his client's private residence. In the late afternoon (exact time unknown) on Saturday, June 22, 2023, Peter Currence convened a three-way with Lindsay McGee and me. During this call I informed Lindsay

McGee about my findings and asked her multiple questions about any electronic items that her estranged ex-husband Justin McGee might have given her or placed in her residence.

Hidden Surveillance Cameras

35. After we ended the call Lindsay McGee searched her residence. At 17:05 EDT her attorney Peter Currence sent me text messages containing photographs of multiple devices that Lindsay McGee believed could be hidden cameras

36. A visual inspection of the device's labels based on the photographs indicated that one of the devices discovered was manufactured by SCS Enterprises. This company's physical address is 6 Fortune Way, Montebello, New York 10901. The company operates two websites, which are https://www.spycameras.com and https://Wi-Fispycameras.com. The device's label also indicated the nomenclature of the camera. The camera was model WF-100PCX. The serial number of the device was 21050298 and the Unique Identification Number (UID Number) was uuuu-197658-bxgmc.

37. A review of the vendor's website indicates that the device discovered was a WF-113. The device features include; power using 110v (standard wall outlet), 1080p HDTV high-definition video, nightvision, Wi-Fi networking and recording capabilities using an embedded Secure Digital (SD) card. The website states that the device can be securely accessed through a remote internet connection using software, which is available for iPhones, iPads, Android devices and personal computers, such as Microsoft Windows. The weblink for this camera is https://Wi-Fispycameras.com/collections/power-adapter-and-chargers/products/copy-of-Wi-Fi-ip-wireless-spy-camera-hidden-in-power-adapter-by-scs-enterprises-1.

38. On Monday, July 24, 2023, Lindsay McGee provided the WF-113 device to Steve Abrams. Mr. Abrams disassembled the device and confirmed that it contained a hidden camera. After the disassembling Mr. Abrams was able to extract the 16GB SD card embedded in the device. According to the manufacturer this SD card is used to store recordings created by the camera. Mr. Abrams confirmed that the SD card contained recordings for the time period between October 9, 2022 and July 22, 2023, at which point Lindsay McGee removed this device from an outlet in her garage. This location gave the person monitoring this covert surveillance camera unfettered access to Lindsay McGee's physical activities in her garage and also allowed someone to listen to her private conversations when the device was triggered by motion detection. There was a gap in the recordings from December 24, 2022 to April 30, 2023.

SCS Enterprises transactional records for Justin McGee

39. On Tuesday, July 25, 2023, attorney Currence transmitted a subpoena to SCS Enterprises to obtain the purchase history for the covert surveillance camera discovered in her residence. SCS Enterprises' subpoena response indicates that the device was purchased by her estranged husband Justin McGee.

40. SCS Enterprises' records confirmed that the spy camera discovered in Lindsay McGee's garage was purchased from the company website. And the company's records indicated that Justin McGee purchased five covert surveillance cameras in 2022 using his PayPal account. These records indicated that all the covert surveillance cameras purchased had audio capabilities. This capability allowed the device to record both audio and video when the covert surveillance camera was activated by motion detection. The monitoring party of the device discovered in Lindsay McGee's residence could not only watch the physical activities of someone, but they could also listen to all private conversations associated with an individual recording.

41. The Arris BGW210-700 (DSL modem) router log files indicate that there had been six different GF-PH130 named devices that have authenticated and connected to the Wi-Fi network in Lindsay McGee's private residence. All of these devices last connected to the Wi-Fi network in July 2023.

42. As previously stated the name GF-PH130 is the nomenclature for a wireless pinhole camera developed by the Chinese company Shenzhen Goodflys Technology Corporation Limited. Each one of these devices had an unique MAC (Media Access Control) address, which linked to the vendor Shenzhen Bilian Electronics Corporation Limited. Shenzhen Bilian Electronics manufactures components used to embed Wi-Fi capabilities in devices, such as covert surveillance cameras. The router log files indicate another seven unique devices embedded with Shenzhen Bilian Electronics components had previously connected to the Wi-Fi network in Lindsay McGee's private residence. Definitive electronic evidence extracted from the Arris BGW210-700 logs confirmed that there have been six GF-PH130 (covert surveillance cameras) in Lindsay McGee's private residence. Circumstantial evidence in the logs suggests that another seven covert surveillance cameras that used the same Wi-Fi components as the GF-PH130 devices existed in Ms. McGee's home between May and July 2023.

43. The WF-113 model of the covert surveillance camera that Justin McGee purchased from SCS Enterprises has a default name of GF-PH130. This was confirmed through a physical analysis of the device, which was obtained from SCS Enterprises by attorney Currence. This camera has remote management capabilities. This camera can be

securely monitored from anywhere in the world by the individual that installed the device. The WF-113 device also has additional security features that make the wireless connection go dormant or silent on a network until a request is made to connect to the device. When a management connection request is made the device wakes-up from its dormant state and fully reconnects to the network. When in this dormant state the camera is still recording both audio and video, which is stored on the device's embedded SD memory card.

44. The purchased records obtained from SCS Enterprises show that the covert surveillance camera that Lindsay McGee discovered in her garage on Saturday, June 22, 2023 was likely purchased in either April 2022 or July 2022. Lindsay McGee has verbally stated that Justin McGee has not been allowed back into her private residence after Saturday, May 28, 2022. So it's likely that the device found has been capturing audio and video recordings at Lindsay McGee's residence since at least May 2022.

45. The Arris BGW210-700 log files show that on Saturday July 8, 2023 at approximately 21:05 EDT a device named "Justins-iPhone" was connected to Lindsay McGee's home Wi-Fi network. This device was using a Private Wi-Fi Address, which is a feature of Apple devices using the mobile operating systems iOS 14, iOS 15 and iOS 16.

46. Since that date this device hasn't reconnected to the Wi-Fi network in Lindsay McGee's private residence. The device named "Justins-iPhone" had to be in extremely close proximity to connect to the Wi-Fi network. Lindsay McGee's private residence is located in a cul-de-sac, so the person using the device named "Justins-iPhone" was either in a vehicle outside her residence or walking near her home. Based on the device naming I can only speculate that this device most likely belonged to Justin McGee. According to the Charleston County Sheriff's Office records posted online Justin McGee was charged on Friday, May 12, 2023 with two felony offenses which were domestic violence in the first degree and burglary in the second degree. Both these offenses occurred at Lindsay McGee's private residence. It is worth noting that several of the covert surveillance cameras with the default names of GF-PH130 went offline the weekend of July 4, 2023. My working professional theory is that these devices were likely removed from Lindsay McGee's residence prior to Friday, July 07, 2023 at 18:43 EDT.

PayPal transactional records for Justin McGee

47. Concerning the SCS Enterprises' purchase records. On Wednesday, July 26, 2023, attorney Currence transmitted a subpoena to PayPal to obtain the purchase history for

the covert surveillance camera purchased by Justin McGee through SCS Enterprises' website. PayPal subpoena response was received on Friday, August 11, 2023.

48. The transactional records for Justin McGee's PayPal account show that he purchased five covert surveillance cameras from SCS Enterprises on three separate occasions in 2022. These purchases were on January 31, 2022, April 25, 2022 and July 26, 2022. The devices purchased were shipped to Mr. McGee's then office address: 125 A Wappoo Creek Drive, Suite A, Charleston, South Carolina, 29412. The payment methods used for these purchases were an American Express card and an account linked to First Arkansas Bank & Trust.

49. A thorough review of the transactional records for Justin McGee's PayPal account showed that he had purchased additional covert surveillance cameras in 2022. On January 24, 2022 he purchased devices from the website knowyournanny.com. The website is operated by Nanny Watch Services, Inc. and Marquis Security Cameras. Both these companies sell covert surveillance cameras. The devices purchased from the website knowyournanny.com were shipped to Mr. McGee's office at 125 A Wappoo Creek Drive, Suite A, Charleston, South Carolina, 29412. The payment method used for this purchase was linked to an account at First Arkansas Bank & Trust. Additional information is required from Nanny Watch Services to identify the specific device purchased. This information is needed to determine the device's capabilities and its design specifications.

50. Justin McGee's PayPal records also indicated that he purchased a covert surveillance camera from Deluxe CCTV Incorporated's website. This purchase was on April 25, 2022, which is the same date that he purchased two covert surveillance cameras from SCS Enterprises. The device purchased was model number BB4KWi-FiSOUNDBAR-04, which is a Soundbar Bluetooth Audio Surround Sound Speaker With 4K UHD Wi-Fi Camera. The vendor's website indicates that the device can be configured to have both night vision and audio. Additional information is required from Deluxe CCTV to determine the purchased device's capabilities and its design specifications. The device in question was shipped to Mr. McGee's office at 125 A Wappoo Creek Drive, Suite A, Charleston,South Carolina, 29412 and was paid for with an American Express card.

51. Justin McGee's PayPal records also indicate that he purchased a growing kit for psilocybin mushrooms, also known as magic mushrooms. Psilocybin mushrooms are considered a Schedule I substance by the Drug Enforcement Administration. The purchase was made on Thursday, July 28, 2022. Third Wave was the vendor that sold the psilocybin mushroom growing kit to Justin McGee. This purchase was shipped to 7312 Eddy Farms Road, Meggett, South Carolina 29449, which is Justin McGee's

residence. The payment method used for this purchase was linked to an account at First Arkansas Bank & Trust.

AT&T Home Internet Bandwidth Records

52. Lindsay McGee gave Peter Currence authorization for me to access her AT&T account. Subsequently Peter Currence gave me written permission on Sunday, Aug 20, 2023 at 17:58 EDT to her AT&T account. On Tuesday, August 22, 2023 a detailed review of the bandwidth records associated with Lindsay McGee's home internet service was performed.

53. The AT&T bandwidth records provide information on the number of gigabytes of data either downloaded or uploaded through Ms. McGee's home internet service. Most consumers have higher download usage than upload usage. This is due to users watching streaming content, such as Netflix or YouTube and accessing sites with high graphical content, such as Facebook or Instagram. The bandwidth records show that several months had substantially more gigabytes being uploaded than other months.

54. One of these anomalies occurred between Friday, August 26, 2022 and Sunday, September 25, 2022. During this period of time the total bandwidth used was 171 gigabytes. The bandwidth associated with downloads for this period was 84 gigabytes. The bandwidth associated with uploads for this period was 88 gigabytes. The latter number indicates that more data was being transmitted out of Ms. McGee's home internet service than being downloaded from the Internet. Data uploads are commonly associated with large file transfers, which includes the streaming of video content, such as from covert surveillance cameras.

55. Another one of these anomalies occurred between Monday, September 26, 2022 and Tuesday, October 25, 2022. During this period of time the total bandwidth used was 127 gigabytes. The bandwidth associated with downloads for this period was 81 gigabytes. The bandwidth associated with uploads for this period was 47 gigabytes. The latter number is fifty-eight percent of gigabytes being downloaded for the same period. This high percentage of uploads is likely associated with streaming video content, such as from covert surveillance cameras being remotely viewed.

56. Another anomaly occurred between Wednesday, October 26, 2022 and Friday, November 25, 2022. During this period of time the total bandwidth used was 202 gigabytes. The bandwidth associated with downloads for this period was 166 gigabytes. The bandwidth associated with uploads for this period was 37 gigabytes. The average bandwidth per month associated with uploads is usually under 20

gigabytes and has been as low as 11 gigabytes, which was between Sunday, March 26, 2023 and Tuesday, April 25, 2023.

57. There was also an anomaly between Saturday, November 26, 2022 and Sunday, December 25, 2022. During this period of time the total bandwidth used was 429 gigabytes. The bandwidth associated with downloads for this period was 396 gigabytes. The bandwidth associated with uploads for this period was 35 gigabytes. The average bandwidth per month associated with uploads is usually under 20 gigabytes and has been as low as 11 gigabytes, which was between Sunday, March 26, 2023 and Tuesday, April 25, 2023.

58. The AT&T bandwidth records strongly indicated that a substantial amount of data was being transmitted from Ms. McGee's network inside her private residence to the Internet. It is my professional opinion that the data being transmitted out of the network was from then covert surveillance cameras. This opinion is based on my experience and on the current evidence, which includes the confirmed presence of a covert surveillance camera in Ms. McGee's home that is mentioned in item 36 of this affidavit and multiple cameras identified in item 41 of this affidavit. There is no disputing that Justin McGee is the individual directly linked to the covert surveillance camera discovered in Ms. McGee's private residence.

Outstanding Subpoenas

59. There is currently an outstanding Apple subpoena requesting login information associated with Lindsay McGee's iCloud accounts, which might confirm that Justin McGee had unauthorized access to her iCloud accounts. There is currently an outstanding AT&T subpoena seeking information on the IP address used on October 30, 2022 to access her iCloud account. On Tuesday, August 15, 2023 there were twenty-one subpoenas relevant to my investigation that are still outstanding. The subpoenas are requesting specific information related to various accounts owned by Lindsay McGee, data related to multiple IP addresses used to access her accounts, records related to Lowcountry PI Services' investigation targeting Lindsay McGee and additional purchasing history linked to Justin McGee's credit card and bank account. The latter information is needed to identify any additional surveillance equipment purchased by Justin McGee.

60. Several of the outstanding subpoenas have been objected to by the respective entities, such as Bank of America, AT&T, Intuit (QuickBooks) and Microsoft. Some of those objections have been resolved. Others, such as Microsoft, are still being negotiated.

61. The AT&T subpoena was to obtain Internet network traffic information for a specific period. This data was needed to identify any remote management connections related to the unauthorized covert surveillance camera(s) placed in Lindsay McGee's residence. AT&T collects network traffic information for quality of service (QoS), law enforcement requests related to illicit activities and national security reasons. This information should be available and will hopefully be produced.

62. The Intuit subpoena was to obtain details related to an unauthorized QuickBooks session on March 13, 2023. An unknown QuickBooks user account linked their account to Lindsay McGee personal Bank of America account. This subpoena was drafted to obtain information about the QuickBooks sessions using the Intuit IP addresses 206.225.202.1, 206.225.203.7, 206.225.203.8 and 206.225.203.9. These IP addresses were listed in the Bank of America IP logs for Ms. McGee account, which were obtained via a subpoena. Any individual accessing QuickBooks at the weblink https://accounts.intuit.com is required to enter valid credentials (User ID and password) linked to an Intuit account. Information related to this unknown account would have a subscriber's name, mailing address of the account subscriber, email address of the account subscriber, phone number of the account subscriber and User ID for the subscriber. Additionally, Intuit collects session information, such as the subscriber IP address for a specific session and any device information (user-agent, device type, geolocation) associated with this access. This information is used for device fingerprinting, which is used for fraud prevention activities at Intuit.

63. The Microsoft subpoena was to obtain access to the Microsoft 365 account for the McGee Law Firm, where Lindsay McGee worked with estranged husband Justin McGee. These Microsoft 365 records could potentially show how many times Justin McGee accessed Lindsay McGee's company email account without her knowledge. Justin McGee is the administrator of the Microsoft 365 account for the McGee Law Firm. As the administrator he had unfettered access to her account with no oversight. Lindsay McGee used her business email lindsay@mcgee-lawfirm.com as a recovery address for these accounts; AT&T, Bank of America, Belk, Discover, Ebay, FNBO (Orvis visa), Gmail, Groupon, Netflix, PayPal, REI, Southern First, Spotify, Ticketmaster and Venmo.

64. The Bank of America account mentioned in Item 34 of this affidavit was linked to an auto loan and a credit card. Lindsay McGee used a different email account when she established a new checking account with Bank of America on Wednesday, November 17, 2021. According to the IP logs obtained from Bank of America an unknown user on Friday, March 13, 2023, linked Ms. McGee's personal bank account to her lindsay@mcgee-lawfirm.com, which she did not have access to on that date.

65. On Monday, June 12, 2023, Justin McGee stated in Item 42 of his affidavit the following: *More importantly, I recently discovered evidence that she purchased marijuana on May 16, 2023 that led me to believe she's been smoking marijuana this whole time and that her boyfriend (Stephen Daniel Fowler) has been providing it to her. On May 16, 2023, at 12:03 p.m., Lindsay sent Fowler $500.00 via Zelle with the message, "Monthly friend fee."*

66. The United States Government passed the Electronic Communications Privacy Act ("ECPA") in 1986. This act was to expand and revise federal wiretapping and electronic eavesdropping provisions. It was enacted to promote "the privacy expectations of citizens and the legitimate needs of law enforcement." The ECPA also makes clear that workplace email is the property of the employer, and employees should not expect privacy when sending, receiving, downloading, uploading, printing or otherwise transmitting electronic messages. Courts have ruled that if an employer owns the computers and runs the computer network, it's generally free to read employee e-mail messages, as long as there is a *"valid business purpose"* for doing so. Justin McGee as the administrator of Microsoft 365 account for the McGee Law Firm had no known business reason to access Ms. McGee's corporate email account lindsay@mcgee-lawfirm.com.

67. Furthermore, it is highly possible that Justin McGee acting as the administrator of Microsoft 365 account for the McGee Law Firm likely intercepted and read other private non-business-related communication of Ms. McGee, such as the one sent by Bank of America on Tuesday, May 16, 2023 to the account lindsay@mcgee-lawfirm.com. Ms. McGee has verbally stated on multiple occasions that she never registered her corporate email account address with Bank of America.

68. The Microsoft subpoena is important, because the email records and access logs might show a pattern of Justin McGee accessing Ms. McGee's corporate email account lindsay@mcgee-lawfirm.com without her direct knowledge or consent.

<u>Summary of Evidence as of 08-25-2023</u>

69. There is definitive evidence showing that Justin McGee purchased covert surveillance cameras in 2022. One of the cameras purchased by Justin McGee was discovered in Ms. McGee's private residence on Saturday, June 22, 2023. Definitive electronic evidence obtained from the AT&T Arris BGW210-700 (DSL modem) router installed in Ms. McGee's private residence shows that six covert surveillance cameras with the same nomenclature were operationally in her home in 2023. The individual that installed these surveillance cameras had to have physical access to Ms. McGee's private

residence to install the cameras and to connect the cameras to Ms. McGee's Wi-Fi network. There is conclusive evidence obtained from Ms. McGee's AT&T account that shows bandwidth anomalies in data being transmitted from Ms. McGee's network to the Internet. These bandwidth spikes are indicative of someone monitoring the covert surveillance cameras from a remote location. The only individual that could have installed and monitored these covert surveillance cameras is Justin McGee, or someone at his direction.

70. There is definitive evidence in the Bank of America IP logs that someone illegally accessed Ms. McGee's banking account on two separate occasions in the month of March 2023. In the intrusion that occurred on Monday, March 13, 2023 at 07:20 PST (10:20 EDT) an unknown subject using an unidentified Apple iPhone and an unidentified computer gained illegal access to Ms. McGee's bank account. The IP address associated with the unidentified Apple iPhone was leased by Wireless Data Service Provider Corporation (WDSPCo) to AT&T Mobility, which is also known as AT&T Wireless. The unidentified computer was connected from an IP Address assigned to the Internet service provider Wide Open West (WOW!). A geographical location search shows that the latter IP address is located in the area of Charleston, South Carolina. During the Monday, March 13, 2023 intrusion into Ms. McGee's banking account the email address lindsay@mcgee-lawfirm.com was added as a contact email. On the date of the intrusion Ms. McGee did not have access to this business email address. The only person that had access to this business email address was Justin McGee, who is the administrator of the McGee Law Firm Microsoft 365 account. On Monday, June 12, 2023, Justin McGee stated in Item 42 of his affidavit the following: *More importantly, I recently discovered evidence that she purchased marijuana on May 16, 2023 that led me to believe she's been smoking marijuana this whole time and that her boyfriend (Stephen Daniel Fowler) has been providing it to her. On May 16, 2023, at 12:03 p.m., Lindsay sent Fowler $500.00 via Zelle with the message, "Monthly friend fee."* Justin McGee is the only individual that would have benefited from adding lindsay@mcgee-lawfirm.com as a contact email to Ms. McGee's banking account. Also during this intrusion the bank transmitted an authorization code (one-time AuthZ code) to a phone number. The contact number on file for Ms. McGee's banking account is 843.xxx.3367. This number is currently assigned to an iPhone 12 Pro Max with the serial number G0NG50GY0D46 in Ms. McGee's possession and to the Subscriber Identity Module (SIM) card in the iPhone 8 that Justin McGee obtained from Ms. McGee in September 2021. Circumstantial evidence suggests that Justin McGee received the authorization code (one-time AuthZ code) sent by Bank of America on Monday, March 13, 2023. There are currently outstanding subpoenas that should confirm this circumstantial evidence.

71. There is definitive evidence contained in Google's IP Logs that shows that the IP addresses listed in the Bank of America IP logs related to the bank intrusion on Monday, March 13, 2023 also compromised Ms. McGee's Gmail account lmcgee9310@redacted. Google's IP Logs cover the period from Friday, November 11, 2022 to Saturday, July 22, 2023. The subpoena was seeking records from Monday, March 01, 2021 to Saturday, July 22, 2023. Google does not maintain Gmail access records for that length of time. The records that Google provided show that someone maintained persistent access to Ms. McGee's Gmail account lmcgee9310@redacted. This access was commonly linked to an unidentified Apple iPhone, which Ms. McGee did not have in her physical possession during the investigation. There is definitive electronic evidence that indicates that the unidentified Apple iPhone continually assessed Ms. McGee's Gmail account prior to a court hearing for her case on Tuesday, June 13, 2023. The unknown subject maintained their access to Ms. McGee's Gmail account for the entire month of May 2023 until Monday, June 12, 2023 at 14:56:34 GMT (09:56:34 EDT), which correlates with the date Justin McGee had his affidavit notarized (time unknown). This unknown subject maintained their access to Ms. McGee's Gmail account until Thursday, June 22, 2023 at 00:15:35 GMT (20:15:35 EDT, which is Wednesday, June 21, 2023). This ending date is significant, because at 17:20 EDT on this date Lindsay McGee's attorney Peter Currence sent an email to Justin McGee's attorneys Jerry Theos and Marie Louise Ramsdale with approximately nine "Notice of Taking Deposition" that were going to be served on Thursday, June 22, 2023. Approximately 5 hours after this email was transmitted to Mr. McGee's attorneys the unknown subject stopped accessing Ms. McGee's Gmail account. Google's IP Logs show that the unknown subject stopped accessing Ms. McGee's Gmail account on Wednesday, June 21, 2023 at 20:15:35 EDT and has not resumed their access since attorney Currence's email was sent to Mr. McGee's attorneys. This circumstantial evidence suggests that Justin McGee is the individual that had unauthorized access to Ms. McGee's Gmail account.

72. The current definitive evidence surrounding the Bank of America intrusion and the multiple Gmail intrusions strongly indicated that Justin McGee is the individual that had unauthorized access to Ms. McGee's accounts. The evidence also indicates that Justin McGee recovered the iPhone 8 given to him by Ms. McGee in September 2021 from one of her iCloud backups. This recovery gave Justin McGee a mirror copy of Ms. McGee iPhone 12 Pro Max on the iPhone 8 in his physical possession. The evidence also suggests that a text message was sent by Bank of America to the number 843.xxx.3367, which was received on both the iPhone 12 Pro Max and on the iPhone 8. Since these iPhones were mirror copies Justin McGee would have had the capabilities to intercept the bank's SMS message and deleted this message on the iPhone 8, which

would have also deleted the message on the iPhone 12 Pro Max in Ms. McGee's physical possession.

73. Based on all the evidence reviewed I strongly believe that Justin McGee had long-term persistent access to Ms. McGee's emails, text messages and data contained in her iCloud account(s). All of Ms. McGee's communications with her attorney Peter Currence either sent or received via text messages on 843.xxx.3367 were most likely intercepted and/or read by Justin McGee. Additionally, all of Ms. McGee's email communications with her attorney Currence using either of her Gmail addresses were also intercepted and/or read by Justin McGee.

74. It is my professional opinion within a reasonable degree of certainty that Justin McGee is the individual that compromised Ms. McGee's Bank of America account and her Gmail account(s). This opinion is based on all the technical evidence analyzed over the course of my preliminary investigation for the McDougall Self Currence McLeod law firm, who is representing their client Lindsay McGee.

Affidavit Status as of 08-25-2023

75. This is a preliminary affidavit and was developed based solely on the data currently available for analysis. As additional data from several outstanding subpoenas becomes available for analysis this affiant will be modified based on that data.

FURTHER THE AFFIANT SAYETH NOT!

John Bumgarner

SWORN TO AND SUBSCRIBED BEFORE ME THIS

29th, **DAY OF** August, **2023.**

NOTARY PUBLIC FOR NORTH CAROLINA

MY COMMISSION EXPIRES: 3 MAY 2025

Kirstin S Reimer Notary Public Buncombe County, North Carolina

John Bumgarner
Asheville, N.C. 28804 • 828-419-4461
https://www.linkedin.com/in/bumgarner

CAREER SUMMARY

- Over 20 years of cybersecurity experience working in corporate, government, consulting and startup environments.
- Well-known in the cyber-security community as a leading cyber-security expert.
- Able to work effectively and in a relaxed manner with everyone from entry-level employees to CEO's and company boards.
- Able to carry out in-depth, technical evaluations of security products and services to determine which are most cost-effective when used together.
- Versed in the use of Big Data and Artificial Intelligence for diagnostic and predictive purposes and able to critically evaluate any claims made for products and services employing those features.
- Knowledgeable in the use of blockchain technologies in various financial markets, including cryptocurrencies, commodity trading, decentralized finance, dark pool trades and smart contracts.
- Expert in every stage of incident handling from the initial technical diagnosis of attack activity to after-incident reporting and public relations.
- Skilled at evaluating and planning every aspect of cyber security as well as physical security.
- Accustomed to working in international contexts that require sensitivity to cultural differences, drawing on work experience in six continents.
- Cool-headed in high-stress situations, as demonstrated by multiple military awards and decorations, including those for heroism.

Skills:

Business Development	Critical Infrastructure	Strategic Research
Governance	Cloud security	Threat Intelligence
Security Architecture	Software Development	Intelligence Analysis
Identity Management	Project Management	Vulnerability Management
Decentralized Finance	Blockchain Technologies	Financial Fraud Investigation

PROFESSIONAL EXPERIENCE

Multiple organizations, United States 2020-2023
Virtual Chief Information Security Officer (vCISO)

- Advised Senior Staff and Board of Directors quarterly on information security program health and industry threat landscape.
- Established application security practice, incorporating threat modeling and secure coding best practices into the Software Development Life Cycle (SDLC).
- Spearheaded phishing and security awareness programs.
- Developed and wrote corporate incident response policy, acceptable use policy and information security policy and standards.

Paxos, New York 2019-2020
Chief Information Security Officer (interim)

- Aligned IT needs with the strategic cyber security direction for all international locations for Paxos' business operations.
- Advised executive management on the appropriate cyber security solutions and technologies to be deployed to secure Paxos' and itBit's products and protect our international customer base.
- Carried out and coordinate all the cyber security and compliance requirements for the Depository Trust & Clearing Corporation (DTCC), NY Department of Financial Services (DFS), the U.S. Securities and Exchange Commission (SEC) and for the Society for Worldwide Interbank Financial Telecommunication (SWIFT).
- Spearheaded the program to establish personally identifiable information (PII) controls and data breach notification requirements for the EU General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) of NY and the Singapore Personal Data Protection Act (PDPA).
- Served as the central point of contact for the Financial Services Information Sharing and Analysis Center (FS-ISAC).
- Reviewed and advised on software designs related to the implementation of blockchain technologies for cryptocurrencies, dark pool trades and smart contracts.
- Provided subject matter expertise on cyber security to both internal and external business & technology teams and articulate risks in business context.

MSCI, New York 2019
Senior Security Advisor to the Global Head of Information Security

- Reviewed and made recommendations on the business continuity plans and procedures for MSCI's global equity index used by securities traders worldwide.
- Evaluated the security controls used to protect the authenticity and integrity of MSCI's global equity index.
- Analyzed and provided insight on the security architectures deployed across this multinational corporation.
- Developed a security roadmap for the cyber security solutions and technologies to be deployed at MSCI between 2020-2022.
- Provided classes on the software development lifecycle and secure coding methods.

Cytenna, California 2015-Present
Chief Product Officer and Co-Founder

- Provided research and development (R&D) activities for the Air Force Research Laboratory, Army Research Laboratory, Defense Advanced Research Projects Agency (DARPA), Department of Defense, Department of Homeland Security, Intelligence Advanced Research Projects Activity (IARPA) and the Naval Research Laboratory.
- Collaborated on techniques to acquire, extract, normalize and categorize datasets compiled from multiple sources.
- Worked on methods to identify patterns and anomalies within complex datasets.
- Collaborated on techniques to forecast activities based on historical events.
- Worked on advanced techniques to visualize complex datasets.

Aeris Capital (Private Equity Firm), Switzerland 2013
Technical Due Diligence Adviser

- Performed due diligence evaluation of a multinational company headquartered in California that specialized in a subset of artificial intelligence.
- Conducted a market review of primary competitors to determine the competitive niches occupied by each competitor and related acquisitions or investments.
- Evaluated intellectual property of the company and its competitors to determine technology overlap, competitive advantage or deficits.
- Reviewed licensing and partnership agreements for intellectual property leakage.
- Wrote comprehensive report highlighting the strengths and weaknesses of this investment opportunity.

Democracy Council, California 2012-2013
Senior Technical Adviser

- Selected and deployed cryptographic software applications.
- Assisted in the production and dissemination of technical manuals written in several languages.
- Expunged all metadata related to geographic location and specific language sets from technical manuals and other project materials.
- Reviewed server logs for attempts to compromise the distribution platform.
- Performed vulnerability assessments and penetration testing of the platform used to distribute the cryptographic applications and manuals.

U.S. Cyber Consequences Unit, Charlotte, NC 2006-2015
Chief Technology Officer and Chief Information Security Officer

- Performed vital strategic and technical research for multiple government agencies.
- Spearheaded high level technical interaction with U.S. Government project stakeholders.
- Developed and co-authored a comprehensive cyber-security checklist, based entirely on field experience, which was downloaded over 100,000 times and used in over 80 countries.
- Helped plan and lead Estonia's first large-scale, nation-wide cyber-security exercise.
- Investigated major cyber campaigns, including the cyber attacks on Georgia during the Russian invasion and wrote the definitive 100-page classified report on that campaign.
- Carried out in-depth investigations of cyber vulnerabilities in critical infrastructure industries, including electric power, natural gas pipelines, healthcare systems, pharmaceutical manufacturing, and natural resource processing.
- Investigated security issues involving the global supply chains used by multiple critical Infrastructure industries.

Cyber Watch, Charlotte, NC 2004-2006
President and Founder

- Performed vulnerability assessments and penetration testing for multiple clients in the Southern United States, to include financial systems, healthcare, and state level government agencies.
- Planned and conducted multiple vulnerability assessments for SunGard Financial Systems for compliance with GLBA and Sarbanes–Oxley.
- Conducted Incident Response activities for an undisclosed healthcare organization and university in the Southern United States.
- Wrote information security standards for all major operating systems and networking devices for a university in the Southern United States.

Lucent Worldwide Services, Charlotte, NC 2004-2006 Senior Security Consultant

- Information security consultant, specializing in Cisco, Microsoft and UNIX environments. Provided strategic consulting services to AT&T, Bell Canada, BellSouth, Sprint, T-Mobile, Verizon and multiple organizations in Europe and South America.
- Performed vulnerability assessments and penetration testing for multiple telecommunication clients, including BellSouth, Sprint and T-Mobile.
- Collaborated on the security architecture for triple play services provided by BellSouth.
- Designed the architecture for a Security Operations Center at Bell Canada.
- Conducted Incident Response activities for an undisclosed telecommunication client and foreign entity.
- Provided subject matter expertise to Bell Laboratories on cybersecurity components being designed and developed.
- Assisted in the development, mentoring and growth of security consultants.

Matrix Network Group (acquired by Dimension Data), Charlotte, NC 2000-2002 Practice Director for Cyber Security

- Worked with other members of the executive team to develop strategic business plans.
- Responsible for driving business development in the cyber security practice.
- Built from scratch a $7 million sales pipeline for cyber security services and products.
- Hired consulting and sales FTE for the cyber security practice.
- Developed career paths for cyber security consultants.
- Implemented a multi-factor identity management solution for Loews Corporation.
- Designed and implemented security architecture for a high-frequency trading firm in New Jersey.
- Planned and managed HIPAA assessments for several health facilities in the Southern United States.

Piedmont Technology Group, Charlotte, NC 1999-2000 Senior Security Consultant

- Information security consultant, specializing in Cisco, Microsoft and UNIX environments. Provided consulting services to BB&T, Bank of America, First Union, Harris Teeter, Krispy Kreme and Wake Forest Baptist Medical Center.
- External member of First Union's UNIX security team.
- Participated in the initial deployment of online banking services for First Union.
- Deployed and secured the online commercial credit systems for First Union.
- Implemented firewalls at Bank of America, First Union, Krispy Kreme and Wake Forest Baptist Medical Center.
- Implemented intrusion detection system for Wake Forest Baptist Medical Center.

- Identified sales opportunity at First Union, which resulted in $2 million in additional revenue.
- Participated in the redesign on the data center at First Union.

IBM Global Services, Cary, NC 1998-1999 System Administrator/Network Security Engineer

- Deployed and maintained Cisco, Microsoft and multiple UNIX platforms.
- Provided end user support for Microsoft and multiple UNIX platforms.
- Performed vulnerability assessments for the computing environment.
- Wrote information security policies and drafted business continuity plans.
- Wrote and maintained information security standards for all major operating systems and networking devices.

U.S. Army (7th Special Forces Group), United States 1987-1998 Senior non-commissioned officer

- Supervised soldiers in multiple environments, including high-stress situations.
- Participated in multilateral operations and strategic operations in Latin America.
- Collaborated on the development and deployment of a classified deployable network using satellite communications.
- Assisted in the deployment of a classified computer network to support American operations in Latin America.
- Performed liaison duties with multiple U.S. Intelligence Agencies, Federal Law Enforcement organizations and members of foreign militaries.
- Security Clearance Top Secret SCI (1988-1998).

U.S. Marines, United States 1980-1987 Non-commissioned officer

- Supervised Marines in multiple environments, including high-stress situations.
- Participated in multilateral operations on six continents.
- Conducted humanitarian operations for foreign nationals in imminent danger.
- Provided physical security for elements of the U.S. nuclear arsenal.
- Security Clearance Secret (1981-1987).

EDUCATION

MA, Information Technology Management, Webster University, Fort Bragg NC
MA, Security Management, Webster University, Fort Bragg, NC
BS, Political Science, Methodist College, Fayetteville, NC

PROFESSIONAL CERTIFICATIONS

2003 - SANS/GIAC Certified Incident Handler (GCIH)
2001 - Systems Security Certified Practitioner (SSCP)
1999 - Certified Information Systems Security Professional (CISSP)

PROFESSIONAL ACCOMPLISHMENTS

2014 - Co-founded BSides Asheville Information Security Conference
2013 - Columnist Dark Reading
2012 - Columnist Information Week
2010-Present - Subject Matter Expert for ISC2 CISSP certification exam

2010-Present - Subject Matter Expert for ISC2 SSCP certification exam
2010 - Co-directed Estonia's first national cyber security exercise
2007-2010 - Senior Research Fellow in Security Studies at the Fletcher School
2009 - Included in the Weapons of Mass Disruption gallery, International Spy Museum
2003-2004 - Board member, High Technology Crime Investigation Association, Carolinas Chapter
2002-2005 - President, North Carolina InfraGard

PROFESSIONAL APPEARANCES

2017 - Speaker, Gulf Information Security conference, Dubai, United Arab Emirates
2016 - Speaker, RSA Conference USA
2016 - Speaker, Gulf Information Security conference, Dubai, United Arab Emirates
2014 - Speaker, World Cyber Security Technology Research Summit, Belfast, Ireland
2014 - Speaker, Cyber Endeavour conference, Naval Postgraduate School
2014 - Speaker, Cyber Defence and Networking Security conference, London, United Kingdom
2014 - Speaker, MEXSEC, Cancun, Mexico
2012 - Speaker, Cyber Defense Forum, Prague, Czech Republic
2012 - Speaker, World Cyber Security Technology Research Summit, Belfast, Ireland
2011 - Speaker, CSIIRW, Oak Ridge National Laboratory
2011 - Speaker, Securitybyte Conference, Bengaluru, India
2010 - Speaker, Cyber Security Summit, Brussels, Belgium
2010 - Panelist, DEF CON 18, Las Vegas, Nevada
2010 - Speaker, Cyber Warfare conference, London, United Kingdom
2010 - Keynote Speaker, Royal United Services Institute, London, United Kingdom
2010 - Speaker, CIA's In-Q-Tel CEO Summit, San Francisco, California
2010 - Speaker, Network Centric Warfare conference, Brussels, Belgium
2010 - Speaker, Nations and cyber warfare, London, United Kingdom
2009 - Speaker Securitybyte/OWASP AppSec Asia Conference, New Delhi, India
2009 - Speaker, Cyber Defense Summit, Dubai, United Arab Emirates
2009 - Speaker, NDIA Cyber Symposium, San Diego, California
2009 - Speaker, Cyber Conflict Policy and Legal conference, Tallinn, Estonia
2008 - Speaker, GovSec conference, Washington, D.C.
2008 - Speaker, Cyber Defense conference, Copenhagen, Denmark
2008 - Speaker, GovNet conference, Washington, D.C
2007 - Guest lecturer, Special Operations/Irregular Warfare Program, Naval Postgraduate School
2007 - Guest lecturer, Center for Homeland Defense and Security, Naval Postgraduate School

ARTICLES AND PUBLICATIONS

2014 - Op-Ed 'When Does a Cyberattack Warrant a Military Response?', NY Times
2014 - 'A Cyber History of the Ukraine Conflict', Dark Reading
2014 - Michelson, M. & Bumgarner, John. Temporal Modeling of Twitter Posting Behavior: An Empirical Study
2014 International Conference on Artificial Intelligence.
2013 - 'A Virus of Biblical Distortions', Dark Reading
2012 - 'When seconds count', Asia Pacific Defense Forum
2012 - 'Securing the Cyber Sphere', Asia Pacific Defense Forum
2012 - 'Decapitating Saudi Aramco with the Sword of Justice', Defence IQ
2011 - 'The Butterfly Effect of Dead Presidents', Dialogo Americas
2011 - 'Cyber Alliances', Asia Pacific Defense Forum

2011 - 'Tech-Savvy Terrorists', Asia Pacific Defense Forum
2011 - 'Tech-Savvy Terrorists', Taiwanese National Defense Digest
2010 - 'Jihad in Cyberspace', Counter Terrorist Magazine
2010 - 'Computers as Weapons of War', Information Operations Journal
2010 - 'Energy Insecurities', Security Management
2008 - 'Electronic Warfare', Intersec Magazine
2008 - 'Russian-Georgian Cyber Conflict of 2008'
2008 - 'Cyber Reconnaissance', Homeland Security Journal
2005 - 'Dialing up new security woes', ISSA Journal
2005 - 'Worms the New Weapons of Mass Destruction', ISSA Journal
2003 - 'Gone in a Flash, Network World
2003 - 'A Hacker Will Be With You Shortly', ISSA Journal
2003 - 'Are USB Flash Drives a security threat', ISSA Journal
2001 - 'Liability Waivers', Security Management Magazine
2001 - 'Red Teams', Security Management Magazine

MEDIA ENGAGEMENTS

2018 - Interviewed on ABC News
2017 - Interviewed on Public Radio International
2017 - Quoted in Deutsche Welle
2016 - Quoted in Christian Science Monitor
2015 - Quoted in The Guardian
2014 - Quoted in Al Jazeera, Bloomberg, Chicago Tribune, Christian Science Monitor, CNBC, Defense One, International Business Times, Newsweek, New York Post, Reuters, Scientific American, The Telegraph, Washington Post
2013 - Quoted in ABC News, Al-Monitor, Christian Science Monitor, Reuters, The Atlantic
2012 - Quoted in Christian Science Monitor, Daily Mail, Reuters, The Globe and Mail
2012 - Interviewed on Newsnight British Broadcasting Corporation
2012 - Quoted in NATOSource Atlantic Council
2012 - Interviewed on National Public Radio
2011 - Interviewed in Reserve Officers Association Magazine
2011 - Quoted in Christian Science Monitor, DNA India, Indian Times, Jerusalem Post, Los Angeles Times, NBC News, Reuters, The Economist, The Verge, Wired
2011 - Interviewed on Southern California Public Radio (SCPR)
2011 - Interviewed on Newsnight British Broadcasting Corporation
2011 - Interviewed on BBC radio Northern Ireland
2010 - Profiled in Jane's Defence Weekly
2010 - Quoted in Bloomberg, CBS News, Fox Business, Reuters
2010 - Interviewed on CBC/Radio-Canada
2009 - Quoted in CNN, Computerworld, The Guardian, Wall Street Journal
2009 - Interviewed on Federal News Radio
2008 - Interviewed on CNN

THE STATE OF SOUTH CAROLINA
In The Court of Appeals

APPEAL FROM CHARLESTON COUNTY
Family Court

Family Court Case No. 2022-DR-10-3072

Appellate Case No.

Lindsay F. McGee, Petitioner,

v.

Justin McGee, Respondent.

AFFIDAVIT OF STEVEN MARC ABRAMS, J.D., M.S.

PERSONALLY APPEARED BEFORE ME, the undersigned, who, being duly sworn, deposes and states the following:

Background

1. My Name is Steven Marc Abrams. I am a licensed Attorney and Counselor at Law, in good standing, in South Carolina, Washington, DC, and New York. I am a member of the South Carolina Bar, The Washington DC Bar, The New York State Bar Association, and the New York State Academy of Trial Lawyers. I am a retired South Carolina State Constable. My field of concentration is digital forensics. I have assisted municipal, county, state, and federal law enforcement agencies and the US Department of Defense and the Department of State with digital forensics investigations for over three decades. For 11 years, from 2008 until 2019, until my

retirement I held a law enforcement commission from the Governor of South Carolina at the request of the United States Secret Service. My office address is 1154 Holly Bend Drive, Mount Pleasant, South Carolina 29466. My office phone number is (843) 813-1996. My full credentials are included in my CV which is appended to this affidavit.

2. I was hired by attorney Peter G. Currence to investigate suspicions of various cyber spying and intrusions into attorney Lindsay McGee's ("Petitioner") online banking and electronic communications in 2022 and 2023. It appeared that her estranged husband, attorney Justin McGee, ("Respondent") had obtained Petitioner's banking records and possessed first-hand knowledge of Petitioner's goings-on that exceeded that which he should have had. As explained below, and further in the affidavit of John Bumgarner, we established direct evidence through our investigation that Respondent secreted multiple spy cameras throughout the separate residence of his estranged wife, Petitioner. These cameras were WI-FI connected and had both audio and video capabilities. Thus, Respondent was able to eavesdrop and intercept all the conversations that Petitioner had within her home, including with her attorney, for over a year. It was also suspected, and confirmed through strong circumstantial evidence during our investigation, that Respondent was reading Petitioner's email and text messages, in a manner that also constituted a series of numerous interceptions of her electronic communications. Finally, it was discovered and confirmed through a mixture of strong circumstantial and direct evidence that Respondent electronically impersonated Petitioner accessing her Bank of America account and thereby changing the email address that was used to communicate her banking statements to an email

account that he exclusively controlled. Thus, he was able to redirect Petitioner's email from the bank to himself where his copying and use of same in the family court litigation between the parties constituted electronic communications interceptions and use of intercepted materials. The conclusion to be drawn from our investigation is that Respondent's entire course of litigation in the family court against Petitioner is based upon his illegal interceptions of her aural and electronic communications, and the use of Petitioner's financial documents obtained by Respondent through illicit means and further interceptions.

CDV Incident part of a pattern and practice to harass Ms. McGee

3. On Friday, May 12, 2023, Respondent broke into the home of Petitioner in a drunken state. When she took out her phone to record him, he attempted to grab her iPhone from her and in the course thereof pushed Petitioner down in front of the former couple's minor children. Respondent was subsequently arrested and charged with first-degree domestic violence and second-degree violent burglary. He was released on $40,000 bond. The charges were later reduced. The takeaway from this incident was Respondent's willingness to break into Petitioner's home illegally if necessary to get something he wanted from her, and in that moment the need to regain control of Petitioner's iPhone at any cost. As we learned during the course of our investigation, Petitioner's iPhones were key instrumentalities used in the multiple interceptions committed by Respondent. It appears that he used Petitioner's older iPhone 8 to gain unauthorized access to her bank account, multiple email accounts, and text message streams. However, the iPhone 8 was not the only means that Respondent employed to

track and spy on Petitioner. We also learned that this was not the only time that Respondent entered Petitioner's home without her consent.

Multiple GPS Trackers used to Surveil and Harass Petitioner

4. For months prior to this CDV incident Petitioner and her boyfriend, whom she started seeing post-separation, found a series of GPS trackers on their personal vehicles. No sooner did they find and remove a GPS tracker from their vehicles when another one was placed on their vehicles to continue the pattern of harassment. In all Petitioner recovered four GPS trackers from her car and her boyfriend found and removed seven trackers from his car. (See Exhibit 4.1 and 4.2, below). The most recent GPS tracker was found on Ms. McGee's car last week on July 25th, 2023. (See Exhibit 4.3, below). During his deposition, Respondent's private investigator admitted that he had been asked to place these devices on Petitioner's car by Respondent, including the last one placed on Petitioner's car in July after Respondent's CDV arrest. The PI stated that Respondent asked for and was given access to the software to monitor these devices himself, except for the last one after the CDV which was monitored by the PI, who reported Petitioner's whereabouts to Respondent several times.

Bugging Investigation - Interceptions of Petitioner's Aural Communications

5. As part of our investigation into possible cyber spying in her residence, the network logs from Petitioner's home router were reviewed by my network forensics colleague, John Bumgarner. John has filed his own affidavit in this matter reporting the details of his network forensics investigation for Petitioner. John's review of the router logs indicated conclusively to a scientific certainty that there had been multiple hidden cameras in Petitioner's residence. Upon this revelation, Petitioner remembered that Respondent

had been in her home prior to when she purchased it, having offered to install "outlet splitters" on some of her electric outlets. Petitioner gathered up these "outlet splitters" and brought them to me on July 24, 2023. It was determined that at least one of them matched a known spy camera seen for sale online and at Amazon. Following proper digital evidence handling procedures, I disassembled the "outlet splitter" and found that it contained a hidden camera. (See Exhibit 2 below.) I documented my examination of the device with a chain of custody and a series of photographs. Inside the unit I found a pinhole camera and a circuit board containing a microSD card. I used FTK imager to make a forensic image of the data contained on the SD card. At the same time, Attorney Currence sent a subpoena to SCS Enterprises in New York State, the company that markets the outlet splitter spy camera that we were examining. I spoke by phone with a representative of the company, Kenneth Lee, who provided us with evidence of Respondent's purchases of five of these spy cameras in three separate orders, on January 31, 2022, April 25, 2022, and July 26, 2022. (See Exhibit 1 below.) The sales receipts document that Respondent paid extra to obtain units that recorded audio in addition to the usual video. Mr. Lee explained that the units connected via Wi-Fi to the Internet and thereby to an app on Respondent's phone that provided real time monitoring and recordings of the audio and video from the hidden cameras. Mr. Lee also provided me with information about a codec and video player application that would allow me to review the video from the SD card. The video from the SD card contained a series of motion activated video sequences dated between October 9, 2022, and July 22, 2023. The camera had only 16 GB of storage on the SD card, and it appears to have wrapped around in a circular buffer after filling the available memory. Thus, it is likely the recording

began before October 10, 2022, and earlier data was overwritten when the recordings exceeded 16 GB. From the videos it could be seen that this camera had been hidden in the back of Petitioner's garage, aimed towards the garage door. From this camera placement Respondent could see in real time anyone entering or leaving the garage of Petitioner's home. Petitioner frequently goes into her garage when she needs to make phone calls outside the earshot of her children, such as to her attorney, and all of these conversations would easily have been recorded and transmitted by the spy camera hidden in the garage. I have not reviewed many of the hundreds of video clips stored to the SD Card, but from what I did review I can confirm that there was video, and audio recorded by the camera, and that Petitioner was frequently recorded in her garage making or receiving phone calls. The five other spy cameras known from the router logs to have been hidden in Petitioners home would to a certainty have made it possible for Respondent to monitor Petitioner's aural communications throughout her home for over a year.

6. There is an interesting gap in the recordings on the SD card from the camera hidden in the garage. There are no video files remaining on the SD card dated between December 24, 2022, and April 30, 2023. On or about March 7, 2023, Respondent entered Petitioner's garage and took her golf cart. Respondent confirmed that to Petitioner after the fact. This is also confirmed circumstantially based on the gap in the recorded video on the SD card. Respondent took the golf cart knowing a camera was hidden in the garage, capturing his entry into Petitioner's home uninvited. He later deleted the video thus creating the gap in the video record to protect his identity. This deletion of recorded video/audio could only be done remotely from the smartphone app that controls the

cameras. Only Respondent had knowledge of the hidden camera in the garage and access to the control software to erase the missing footage. So, only Respondent could have erased the video to conceal the theft of the golf cart.

7. I performed a forensic analysis of the SD card data attempting to locate the deleted video sequences from the gap period. I was able to confirm that there were many deleted folders and video files, but because they had been wiped (overwritten with a repeating pattern), I was not able to recover the video content or the metadata.

Respondent's Pleadings Based Largely on Knowledge Gained from Interceptions.

8. I have reviewed Respondent's Complaint and affidavit filed in the family court. Much of the material that forms the basis of the Complaint and affidavit consists of allegations that could only be obtained by having eyes and ears inside Petitioner's home in the period of time when Respondent was known to have had the six spy cameras secreted in Petitioner's home. Other allegations in the Complaint and affidavit specifically refer to material contained in Petitioner's electronic communications. (See Complaint Paragraphs 12-15, and Affidavit of Justin McGee, Paragraphs 24. a. through f., k. through m.)

Electronic Impersonation and Interception investigation – Bank of America

9. It was learned through a series of subpoenas to Google, Apple, Bank of America, AT&T that based upon IP address history and other identifying information further explained in Mr. Bumgarner's affidavit that there is sufficient circumstantial evidence to show that Respondent used Petitioner's Apple iPhone credentials and her iPhone 8 that was in Respondent's possession at the time to gain access to her account at Bank of America, and thereby to change the contact email address to one that he

controlled exclusively. He thereafter received banking statements for Petitioner's Bank of America account, including one that he gave to his attorney that was filed as evidence in the family court. This email forwarding rule at Bank of America to an email account that Respondent alone had access to constituted an interception of Petitioner's electronic communications. (See *U.S. v. Councilman*, 418 F.3d 67 (1st Cir. 2005), *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010), and *Epstein v. Epstein*, 843 F.3d 1147 (7th Cir. 2016)). The manner in which Respondent received Petitioner's Bank of America statement that was filed in the family court is direct evidence of the illegal interception of her electronic communications from the bank and proves his direct involvement in the underlying bank fraud scheme. The use of this intercepted email as evidence in the family court constituted an illegal "use" of this material in violation of the South Carolina Homeland Security Act.

Investigation into Interception of Petitioner's email

10. We also suspected that Petitioner's email and text messages had been compromised and sent subpoenas looking for evidence of account intrusion. As Mr. Bumgarner explained in his affidavit the information obtained from these subpoenas provided evidence that someone accessed Petitioner's Gmail account repeatedly without her knowledge or consent. There is strong circumstantial evidence that the "someone" is Respondent based on the use of the same IP address to intercept Petitioner's Gmail and orchestrate the bank fraud scheme that is tied to Respondent through his filing of the intercepted bank records in family court.

Opinions

11. The investigation conducted by Mr. Bumgarner and me confirmed that Respondent conducted a sophisticated and illegal surveillance of Petitioner for more than a year that included GPS tracking of her every move, aural interceptions, video surveillance of Petitioner in her home using at least six spy cameras hidden throughout her home, and the interception of Petitioner's electronic communications including email and text messages. Additionally, Respondent electronically impersonated Petitioner to gain control of her business banking account and intercepted her statements and other electronic communications from her financial institution. Further, it appears that Respondent used all this illicitly intercepted intelligence regarding Petitioner as the basis for his pleadings in the family count in multiple violations of the South Carolina Homeland Security Act. As required by law I have shared my direct evidence of Respondent's wiretapping and related illegal activities with the appropriate law enforcement authorities.

FURTHER THE AFFIANT SAYETH NOT!

Steven M. Abrams

Steven Marc Abrams, J.D., M.S.

SWORN TO AND SUBSCRIBED BEFORE ME THIS 29th, DAY OF August, 2023.

Samantha J Maiale

NOTARY PUBLIC FOR SOUTH CAROLINA
MY COMMISSION EXPIRES: March 18, 2024

EXHIBITS

Exhibit 1 - Sales receipt from SCS Enterprises for five spy cameras purchased by Justin McGee and shipped to his office.

SCS ENTERPRISES

Order #2536
January 31, 2022

SHIP TO

Justin McGee
125 A Wappoo Creek Dr
STE A
Charleston SC 29412
United States
(843) 847-1502

BILL TO

Justin McGee
125 A Wappoo Creek Dr
STE A
Charleston SC 29412
United States

ITEMS	QUANTITY
WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) DOWN / Add Audio / 32GB WF-113D-A-32	1 of 1

Thank you for shopping with us!

SCS Enterprises
6 Fortune Way, Montebello NY 10901, United States
info@spycameras.com
wifispycameras.com

SCS ENTERPRISES

Order #2628
April 25, 2022

SHIP TO

Justin McGee
McGee Law Firm
125A Wappoo Creek Dr, STE A
STE A
Charleston SC 29412
United States
(843) 847-1502

BILL TO

Justin McGee
McGee Law Firm
125A Wappoo Creek Dr, STE A
STE A
Charleston SC 29412
United States

ITEMS		QUANTITY
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) Straight / Add Audio / 16GB WF-113-A	1 of 1
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) DOWN / Add Audio / 16GB WF-113D-A	1 of 1

Thank you for shopping with us!

SCS Enterprises
6 Fortune Way, Montebello NY 10901, United States
info@spycameras.com
wifispycameras.com

SCS ENTERPRISES

Order #2747
July 26, 2022

SHIP TO

Justin McGee
125A Wappoo Creek Dr
Charleston SC 29412
United States
8438471502

BILL TO

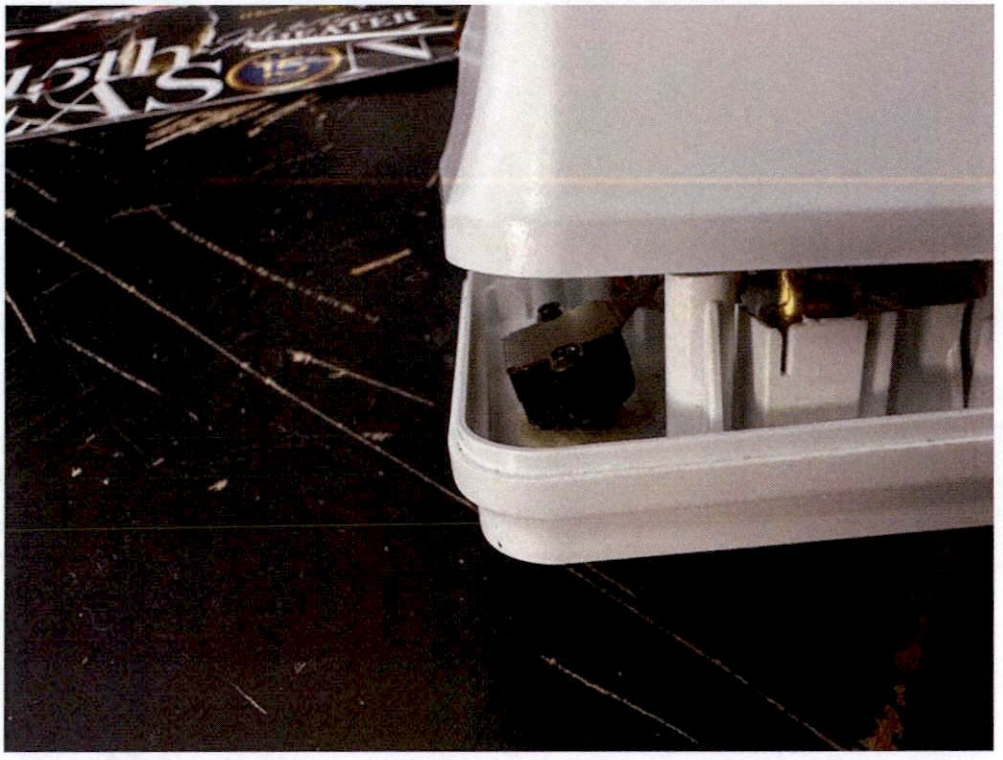
Justin McGee
125A Wappoo Creek Dr
Charleston SC 29412
United States

ITEMS		QUANTITY
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) DOWN / Add Audio / 16GB WF-113D-A	1 of 1
	WF-113 : Sony 1080p Chip Super low light Wireless Spy Camera with WiFi Digital IP Signal, Recording & Remote Internet Access (Camera Hidden in 3 AC Outlet with Dual USB Charging Port Wall Charger)) Straight / Add Audio / 16GB WF-113-A	1 of 1

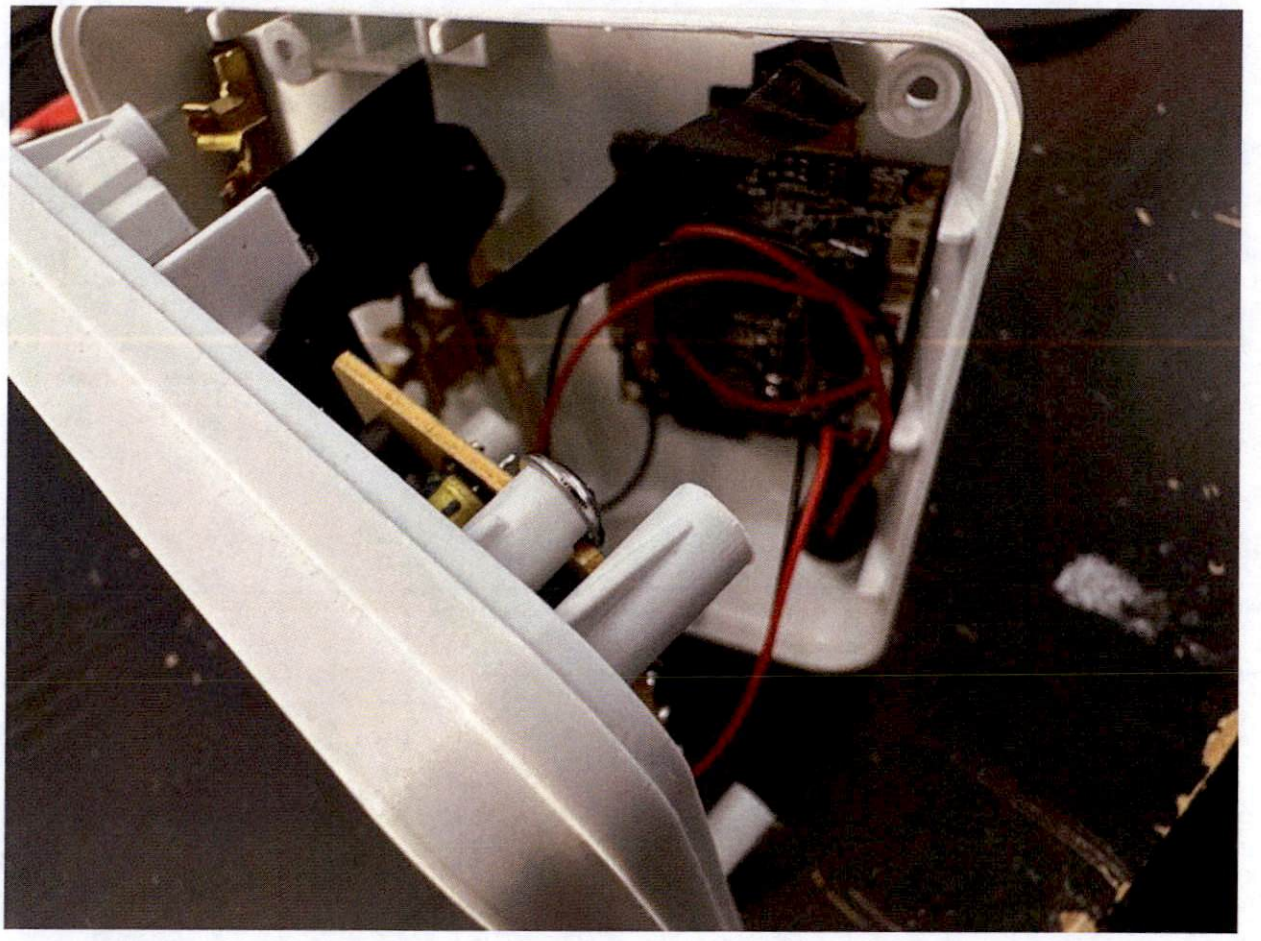
Thank you for shopping with us!

SCS Enterprises
6 Fortune Way, Montebello NY 10901, United States
info@spycameras.com
wifispycameras.com

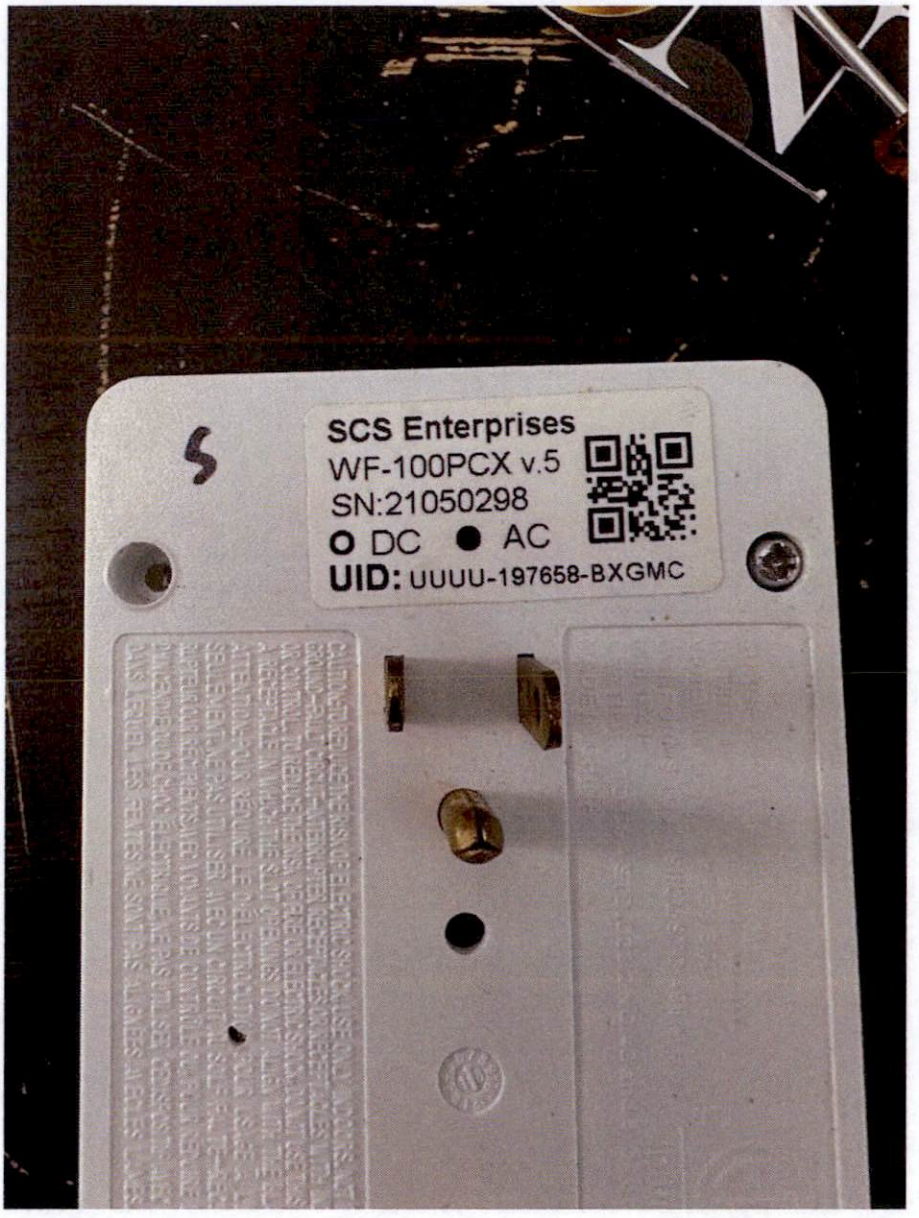
Exhibit 2 – Photos of Spy Cam in USB charger and disassembled to reveal SC Card containing videos of victim and her children coming and going from victim's garage.



2.1 - SONY camera secreted inside the SCS Enterprises USB charger spy camera.

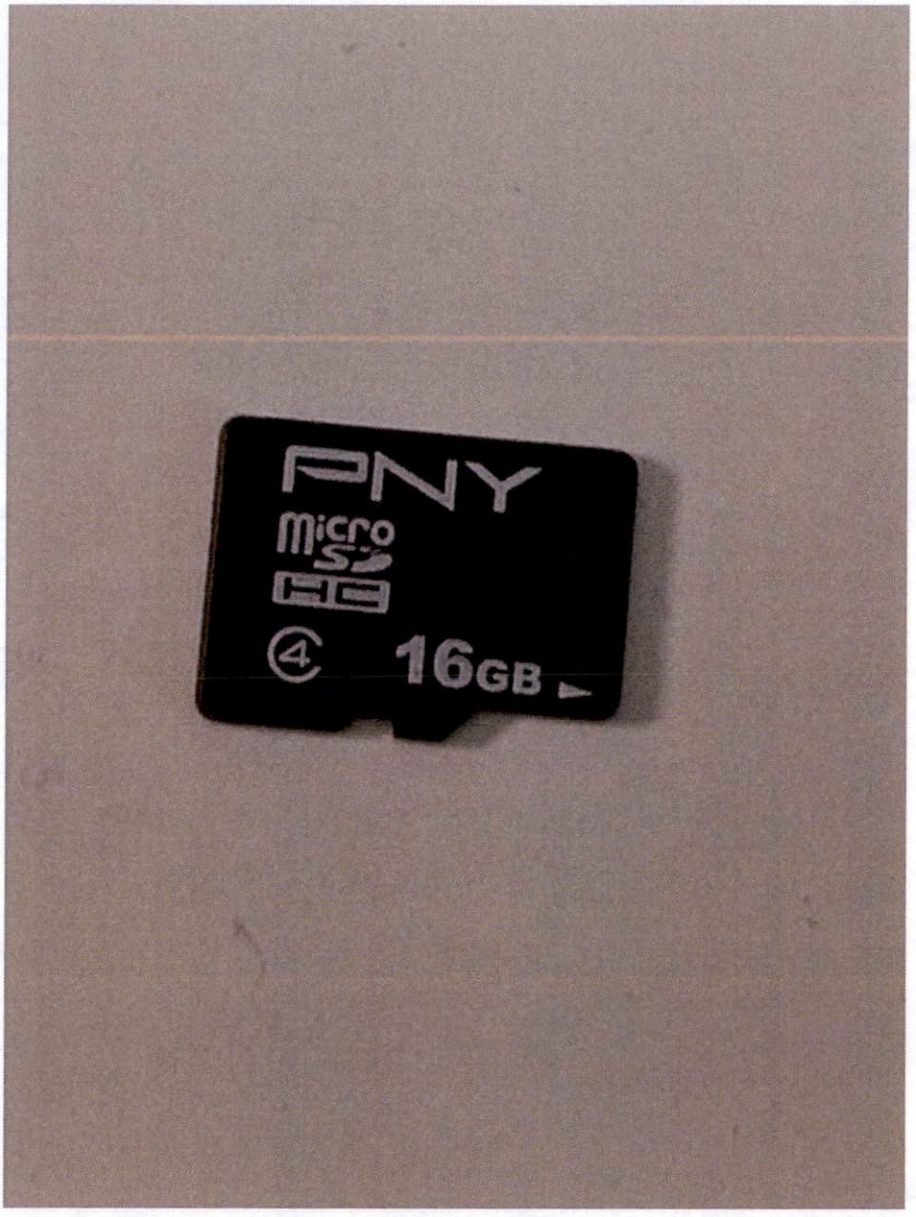


2.2 - WIFI and Recorder circuit with SD Card installed.



2.3 - Product label on back of spy camera.

2.4 - Front of spy camera. Hidden camera is behind the round opening on top right.



2.5 - 16 GB SD card removed from the Wi-Fi and recording module inside the spy camera.

Video stored on the SD card in raw .264 format, and showed the recording was of audio and video captured in victim's garage.

3. – Additional chargers removed from victim's home that need to be examined for hidden cameras

4.1 - First group of GPS trackers removed from victim's car.

4.2 - Second group of GPS trackers removed from Victims' vehicles.

4.3 - Most recent GPS removed from Ms. McGee's vehicle on July 25, 2023.

Four GPS trackers were removed from Ms. McGee's personal vehicle. Seven GPS trackers were removed from the personal vehicle of Ms. McGee's boyfriend.

APPENDIX A.

Steven M. Abrams, J.D., M.S.
Curriculum Vitae

Steven M. Abrams, J.D., M.S.
Attorney, Digital Forensics Examiner and Instructor
1154 Holly Bend Drive
Mount Pleasant, SC 29466
843-216-1100
Steve@AbramsForensics.com

Curriculum Vitae

My key practice areas are Electronic Privacy, Digital Forensics and e-Discovery, and Computer Law.

Education

2016 -Techno Security 2016, Computer Forensics Training Seminar, Myrtle Beach, SC, June 5-8, 2016

2014 -Georgia Bureau of Investigations, Internet Evidence Finder Forensics Training, Decatur, Georgia, February 2014

2013 -Techno Security 2013, Computer Forensics Training Seminar, Myrtle Beach, SC, June 2-5, 2013

2012 -Techno Security 2012, Computer Forensics Training Seminar, Myrtle Beach, SC, June 3-6, 2012

2011 -November 9-12: EnCase 7 Training, Salt Lake City, UT
-November 6 – 9: Paraben Forensics Innovations Conference, Park City, UT
- South Carolina Assoc. of Legal Investigators (SCALI) Annual Training Seminar, May 2011
- April 7, 2011: SC Electronic Crime Task Force Quarterly Meeting and Training

2010 -Techno Security 2010, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2010

2009 - Cellebrite Mobile Device Forensics Certification (CCMDE), SEMAR, Mexico City, Mexico
-SCALI Annual Training Seminar, May 2009

2008 - South Carolina Basic Constable Training, Tri-County Technical College / SC Criminal Justice Academy, October – November 2008
- Commissioned as a South Carolina State Constable (LEO) on November 20, 2008.
- Techno Security 2008, Computer Forensics Training Seminar, Myrtle Beach, SC, June

2007 - Charleston School of Law, Charleston, SC, Juris Doctor (J.D. - Magna Cum Laude)

- GMU2007 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2007 (40 CEU HTCIA)
- Techno Security 2007, Computer Forensics Training Seminar, Myrtle Beach, SC, June

2006 - University of Aberdeen, School of Law, Kings College, Old Aberdeen, Scotland in collaboration with the University of Baltimore Law School Summer Law Program in Comparative Criminal Procedure and UK Business Entities & Taxation
- Techno Security 2006, Computer Forensics Training Seminar, Myrtle Beach, SC, June
- SCALI Annual Training Seminar, May 2006

2005 - SCALI Annual Training Seminar, May 2005
- SCALI Fall Training Seminar, October 2005

2004 - Access Data Advanced Windows Forensics, June 23-25, 2004, New York City. (24 Credit Hours)
- SCALI Annual Training Seminar, May 2004 (10 CEU)

2003 - GMU2003 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, George Mason University, Fairfax, VA. Aug.2003, (40 CEU HTCIA)
- Techno Security 2003, Computer Forensics and Security Conference (24 CEU)
- SCALI Annual Training Seminar & PI Training Seminar (16 CEU SLED)

2002 - SCALI Annual & Fall Training Seminars (16 CEU SLED)
- GMU2002 Computer Forensics Symposium, Regional Computer Forensic Group of the High Technology Crime Investigation Association, Fairfax VA, Aug. 2002, (40 CEU HTCIA)
- Access Data Computer Forensic Boot Camp, North Carolina Justice Academy, Edneyville, NC (24 CEU)

1992-1994 Microsoft Internet Developer Workshops NY, NY

1992-1993 Novell NetWare CNE Training, IBM Skills Discovery, Jericho NY

1984-1985 Microcomputer and Electronics Engineering, Hofstra University, Hempstead NY

1982-1983 Ph.D. Studies, Faculty Fellowship, Columbia University, Graduate School of Arts & Sciences

1981-1982 Columbia University, College of Physicians & Surgeons, Master of Science (M.S.)

1977-1981 Allegheny College, Meadville PA, Bachelor of Arts (B.A.) (Psychology - Computer Science)

Professional Licenses

Current

Licensed Attorney in South Carolina
Licensed Attorney in District of Columbia
Licensed Attorney and Counselor at Law in New York

Previous

Licensed as a Private Investigator in South Carolina and New York (2002-2008), South Carolina State Constable (Sworn, 2008-2019).

Experience (Selected)

2016 – Present, Senior Attorney, Abrams Cyber Law & Forensics, LLC. Mount Pleasant, SC 29466. Concentration on Electronic Privacy and Defamation Cases, Electronic Discovery, and Digital Forensics.

2018 - Continuing Legal Education Instructor, ***Electronic Privacy Violations during Divorce: Legal and Ethical Guidelines for Family Law Practitioners,*** SC Bar, Columbia SC (February 21, 2018).

2016 – Continuing Legal Education Instructor, ***Smartphones as evidence for Personal Injury Cases***, NBI, Charleston SC (December 8, 2016).

2011 – 2016 Sole Practitioner Abrams Law Firm, PC. Mount Pleasant, SC 29466

2011 - Digital Forensics Instructor / Investigator, H-11 Digital Forensics / United States Embassy, Tirane, Albania.

2010 – Facilitator, Instructor, Annual In-Service Legals and CDV Training (SLED), Lowcountry Constable Association.

2009 – Speaker, South Carolina Association for Justice, Hilton Head, SC (August 6, 2009) Topic: Civil Discovery of E-mails after *O'Grady*

2009 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Digital Forensics Instructor/Investigator, H-11 Digital Forensics / United States Embassy, Mexico City, Mexico.

2008 – Faculty, SC Bar Convention – Family Law Section CLE

2008 – 2011 Shareholder, Abrams Millonzi Law Firm, P.C., Mount Pleasant, SC 29464

2007 - Presenter, "E-Discovery: Definition, FRCP Changes and Application CLE",NBI, Charlotte, NC, December 19, 2007

2007 - Digital Forensics Instructor/Investigator, H-11 Digital Forensics, United States Embassy, Mexico City, Mexico

2007 - Presenter, "Civil to Criminal: Collaborative Computer Forensics Investigations between PIs and Law Enforcement",GMU2007, August 9th & 10th, 2007

2007 - Presenter – "A South Carolina Lawyer's Roadmap to Navigating the New Federal E-Discovery Rules," The South Carolina Bar (CLE Division), April 13, 2007.

2006 - Presenter – "Typical Internet Sexual Activity and its Detection", Family Law CLE, The South Carolina Bar (CLE Division), November 2006.

2006 - Instructor, "3-day Hands-on Computer Forensics Workshop", Trident Technical College, N. Charleston, SC, CLE accredited by The South Carolina Bar, January 2006.

2005 - Lecturer, "Computer Forensic Introduction", Trident Technical College, CLE accredited by South Carolina Bar and CEU / In-Service hours for PIs / LE by SLED.

2001 - Present Steve Abrams & Company, Ltd. (dba Abrams Computer Forensics)
Licensed Private Investigator, Computer Forensics Examiner

1998 - 2001 Steve Abrams & Company, Ltd. Mt. Pleasant, SC, President

1996 - Democratic National Committee, Instructor - Southeast and Northeast Regional Schools for Congressional Campaign Managers.

1995 – 1999 Direct Marketers of Charleston Mt Pleasant, SC, Partner
Co-owner of Political Database Marketing Company and full service political print shop.

1994 - 1995 The Software Studio Mt Pleasant, SC, Owner
Owner of software development company that developed database applications for the Newspaper publishing industry.

1992-1993 Town of North Hempstead, Manhasset, NY, Deputy Commissioner of Finance

1986 - 1992 Digitron Telecommunications, Inc., Huntington, NY, Director of R&D

1984 - 1986 Computer Associates International., Islandia, NY, Senior Systems Programmer

1983 Contel Information Systems Division. Great Neck NY, Software Engineer
(Developed the first Network Forensics Applications for the DoD

Recent Publications

Steven M. Abrams, Knowledge of Computer Forensics Is Becoming Essential for Attorneys in the Information Age, 75 N.Y. St. B. Assn. J. 8, 15 (Feb. 2003).

Steven M. Abrams, Knowledge of Computer Forensics, Essential for 21st Century Private Investigators, 16 PI Mag. 46, 59 (October 2003).

Professional Awards & Honors

2008 – Member, SLED Ad Hoc Committee on Computer Forensics

2007 – CALI Excellence for the Future Award, Aviation Law, Charleston School of Law, Fall 2006

- CALI Excellence for the Future Award, Interviewing, Counseling & Negotiation, Charleston School of Law, Fall 2006

- CALI Excellence for the Future Award, Insurance Law, Charleston School of Law, Fall 2006

_ Dean's List, Charleston School of Law, Fall 2006, Spring 2007.

2004 - "2004 SCALI Investigator of the Year"

2003 - Member, SLED Private Investigations Business Advisory Committee

Professional Associations

Member, Institute of Electrical and Electronics Engineers - IEEE
Member, Lowcountry Constables Association - LCA

Bar Association Memberships

Admitted to practice in **South Carolina, District of Columbia, and New York**.

Compensation

I receive $425 per hour, plus mileage, travel and lodging expenses, for all Computer Forensics services and for depositions and trial testimony.

Previous Expert Testimony

I have completed over 1250 computer forensics investigations; the overwhelming majority of cases were settled and did not require me to testify.

South Carolina cases in which I was qualified in court as an expert are:

Hillburn v. Hillburn, (2001-DR-08-2354);
Smith v. Smith, (2001-DR-22-212);
Natale v. Natale, (2003-DR-10-775)
Berda v. Berda, (2003-DR-10-1899);
Murphy v. Murphy (2004-DR-10-1510) and
Overstolz v. Fountain of Youth Wellness Centers LLC (2003-CP-10-000761).
Gitter v. Gitter (2008-DR-10-2865)
Ricigliano v. Ricigliano, (2009-DR-18-0102)
Edwards v Junevicus, (2010-DR-10-4736)
BTM Machinery Inc. v. Michael J. Finley *(2013-CP-10-4366)*
Cherry v Cherry (2014-DR-10-95)
Whitfield v. Schimpf and Sweetgrass Plastic Surgery, *LLC (Case No. 2017-CP-10-2758)*

I was qualified as a testifying expert on digital forensics in federal court in the South Carolina Federal District Court

UHLIG, LLC, V JOHN ADAM SHIRLEY, *(CIVIL ACTION NO.. 6:08-1208-HFF) GREENVILLE DIVISION*
UNITED STATES OF AMERICA V. BRANDON DANIELS *(CRIMINAL, 2021) CHARLESTON DIVISION*

I have also prepared expert's reports under Federal Rule 26(a)(2)(B) for the following federal civil suits filed in the United States District Court for the District of South Carolina:

Lumpkin v. Bennani, (Civil Action No. 2:03-2904-23), and
Miller v. American LaFrance Corp. (Civil Action No. 2:04-1668-23)
Microsoft v. **BWC Products Inc.** (Civil Action No. 2:06-CV-2023-CWH)
Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al. (Civil Action No. 2:07-CV-00673-PMD)
Mainfreight v. John Marco, et al., (Civil Action No. 9:cv00563 JFA)

And in the United States District Court for the Southern District of New York:
UNITED STATES OF AMERICA v. KEITH RANIERE (also known as "VANGUARD") and ALLISON MACK (Case 1:18-cr-00204-NGG-VMS)

I was appointed the Court's Expert in United States District Court, District of South Carolina, Rock Hill Division:

The Travelers Home and Marine Ins. Co. v. Pope, C/A No.: 0:10-cv-1688-JFA

I was qualified as a testifying computer forensics expert in North Carolina courts in: ***Hollins v. Lightfoot.***

In addition, I have been deposed in the following matters over the past ten years:

Thomas & Assoc. v. Christopher Humphreys *(Case No. 2018-CP-10-0455)*
Catherine Cope v. Wells Fargo Bank N.A., Century 21 Properties Plus, and Jim Bailey, individually; *(Case No.: 2018-CP-18-00112)*
Rick Gray v. Church Mutual *(2017)*
Calandra v. Calandra *(2004-DR-10-2675)*
McLernon v. McLernon *(2003-DR-10-3090)*
White v. Cassidy *(*2004-DR-08-256)
Khoury v. Noce (2006-CP-10-001830)
Quala Systems, Inc, et al., v. Bulkhaul USA, Inc., et al. (Civil Action No. 2:07-CV-00673-PMD)
Mainfreight v. John Marco, et al., (Civil Action No. 9:cv00563 JFA)
Beard v. Dunn & Dixon-Hughes et al, (Case No. 2010-CP-08-0776)
UHLIG, LLC, V JOHN ADAM SHIRLEY, *(CIVIL ACTION NO.6:08-1208-HFF)*
ALTMAN, ET AL. V. FIRST CITIZENS BANK AND TRUST COMPANY *(2012-CP-34-0124)*

(Revised: January 29, 2023)

THE STATE OF SOUTH CAROLINA
In the Court of Appeals

RECEIVED
AUG 30 2023
SC Court of Appeals

APPEAL FROM CHARLESTON COUNTY
Family Court

Case No. 2022-DR-10-3072

Justin McGee,…….. .....Respondent

v.

Lindsay McGee, ……Petitioner

PROOF OF SERVICE

I certify that I have served the MOTION TO SUPPRESS EVIDENCE on Respondent, by email and by depositing a copy of it in the United States Mail, postage prepaid on August 29, 2023, addressed below:

Mr. Jerry N. Theos
Theos Law Firm, LLC
11 State Street
Charleston SC 29401

Ms. Marie-Louise Ramsdale
Ramsdale Law Firm
1476 Ben Sawyer Blvd., Suite 5
Mt. Pleasant, SC 29464

Ms. Elizabeth J. Stringer
Stringer Law
753 Folly Road
Charleston, SC 29412

The Honorable Alice Anne Richter
Chief Administrative Judge
Charleston County Family Court
100 Broad Street
Charleston, SC 29401

Peter G. Currence
McDougall, Self, Currence & McLeod, LLP
791 Greenlawn Drive, Suite 4
Post Office Box 90860
Columbia, SC 29290-1860
(803) 776-3130

ATTORNEYS FOR PETITIONER

August 12, 2023

McDougall | Self | Currence | McLeod

John O. McDougall*†
Peter G. Currence
Ryan A. McLeod*‡
Alyssa H. Richardson
R. Jason Hall^
Adam Pickworth

Of Counsel: Michael W. Self

791 Greenlawn Dr., Suite 4, Columbia, SC 29209-2641
P.O. Box 90860, Columbia, SC 29290-1860
(803) 776-3130 phone; (803) 961-6653 fax

21 East Calhoun St., Sumter, SC 29150-4315
P.O. Box 2197, Sumter, SC 29151-2197
(803) 778-5062 phone; (803) 778-6908 fax

August 30, 2023

Honorable Jenny Abbott Kitchings
Clerk, South Carolina Court of Appeals
1015 Sumter Street
Columbia, SC 29211

RECEIVED
AUG 30 2023
SC Court of Appeals

RE: Justin McGee v Lindsay McGee
Case # 2022-DR-10-3072

Dear Ms. Kitchings:

Enclosed please find the MOTION TO SUPPRESS EVIDENCE in regard to the above referenced matter. Please return a filed stamped copy to me. I am also enclosing a CERTIFICATE OF SERVICE and our firm's check in the amount of $50.00.

With kind regards.

Sincerely,

PETER G. CURRENCE

PGC:lr
Enclosure
Cc: Ms. Lindsay McGee (via Email Only)
Mr. Jerry Theos (via Email Only)
Ms. Marie-Louise Ramsdale (via Email Only)
Ms. Elizabeth J. Stringer (via Email Only)