❒ Original ❒

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
information associated with Sunbadger.com that is stored at premises controlled by Slack Technologies

Case No. 23-M-544 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

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

See Attachment A

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

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before 1-4-24 *(not to exceed 14 days)*

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

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

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

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

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

Date and time issued: 12-21-23. 9:50 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

U.S. Magistrate Judge Stephen C. Dries
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

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

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to all information associated with the account identified as follows (the "SUBJECT ACCOUNT") that is within the possession, custody, or control of **Slack Technologies**, a company that accepts legal process at 500 Howard Street, California 94105, regardless of where such information is stored, held, or maintained:

- Sunbadger.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Slack Technologies (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 15, 2023, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The contents of all communications associated with the account from January 1, 2021 to August 14, 2023, including stored or preserved copies of communications sent to and from the account, draft communications, the sender and recipient associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. The types of service utilized;

4. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **fourteen (14) days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1341 and 1343, those violations involving Sun Badger Solar, Kristopher Sipe ("Sipe"), and Trevor Sumner ("Sumner"), and occurring after January 1, 2021, including but not limited to the following:

(a) Communications between Sumner, Sipe, Debra Mahoney, Kevin Armel Martin, Nick Landauer, Benjamin Ganje, and other Sun Badger Solar employees regarding payment terms for customers, cash deposits, installation timelines and delays, and ongoing investigations into the business's trade practices.

(b) Records that reveal the state of mind of Sun Badger Solar employees and principals with respect to the accuracy or falsity of representations being made to customers and other aspects of the crimes under investigation.

(c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to signing solar panel contracts, upper-management meetings, employee trainings, or the company's financial condition, including records that help reveal their state of mind and whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits,

and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

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

information associated with Sunbadger.com that is stored at premises controlled by Slack Technologies

Case No. 23-M-544 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

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

See Attachment A

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

See Attachment B

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

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

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1341 and 1343	Mail and Wire Fraud

The application is based on these facts:

See Affidavit

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

Ashley Gentle
Applicant's signature

FBI SA Ashley Gentle
Printed name and title

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

Date: 12-21-23

Stephen C. Dries
Judge's signature

City and state: Milwaukee, Wisconsin

U.S. Magistrate Judge Stephen C. Dries
Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ashley Gentle, being first duly sworn, hereby depose and state a follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises owned, maintained, controlled, or operated by Slack Technologies ("Slack"), an electronic communications service and/or remote computing service provider headquartered at 415 Mission Street, 3rd Floor, San Francisco, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), to require Slack to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent ("SA") for the Federal Bureau of Investigation ("FBI") currently assigned to the Milwaukee Field Division. I have been employed as a SA with the FBI since February 2023. I have received basic federal law enforcement training, including the training at the FBI academy, as well as other specialized federal law enforcement training. I have participated in the investigation of numerous criminal matters. I have used many investigative techniques in furtherance of such investigations. I have interviewed and operated informants, conducted searches and interviews, and have conducted physical and electronic surveillance. In my experience as a law enforcement officer, I have assisted in investigations, which have resulted in the issuance and execution of search warrants resulting in the seizure of evidence, and the arrest

of individuals to include those involved in financial fraud, and other violations of federal criminal law.

3. I have knowledge of the following information based on my own observations and investigation as well as information that I have learned from other law enforcement officers, to include but not limited to, verbal discussions with other law enforcement officers named in this affidavit. Because this affidavit is being submitted solely for establishing probable cause to obtain warrants, I have not included each and every fact known to your affiant concerning this investigation. I have set forth facts necessary to support the authorization of the requested search warrant.

IDENTIFICATION OF THE PROPERTY TO BE EXAMINED

4. The property to be searched is the Slack account: Sunbadger.com (hereinafter the "Target Account"). The applied-for warrant would authorize the examination of the Target Account for the purpose of identifying electronically stored data, particularly described in Attachment B.

BACKGROUND ON SLACK

5. Based on a review of information provided by Slack regarding its services, information provided by other law enforcement officers, and/or my training and experience, I am aware of the following information about Slack.

6. Generally speaking, Slack is a chat tool used by businesses for communication among employees.

7. Slack, an acronym for "Searchable Log of All Conversation and Knowledge," is a cloud-based application that hosts team-based collaboration tools and services. Slack offers persistent chat rooms, known as "channels," that are organized by topic, as well as private groups

and direct messaging. Slack integrates with a large number of third-party services and integrations, including Google Drive, Dropbox, and Box, among others.

8. Slack claims to simplify team-based communications by creating a shared workspace where conversations are organized and accessible by members. Slack allows users to join workspaces through specific URLs or invitations sent by the team administrator or owner. This shared workspace includes an archive of all past conversations related to Slack teams and communication channels. Slack features a searchable archive of team conversations and work. Slack offers users the ability to create and then manage channels for a project, team, or topic, with Slack retaining that data—including messages—for the life of a particular Slack team.

9. Slack advertises six different types of communication mediums on its website:

a. Public Channels: These are channels for projects, groups, and topics that are open to anyone on a particular team. Slack advertises that messages on these channels are archived and accessible by search.

b. Private Channels: Slack states that these channels are for sensitive or confidential conversations. Private channels contain conversations between a group of invited members. Messages are then searchable and accessible only to members who have been invited.

c. Direct Messages: Slack claims that this type of message is on a "one to one" or "small group" basis. Slack also states that direct messages can be converted by users to private channels for longer-running topics.

d. Slack Connect: According to Slack, Slack Connect allows for integrated communication between clients, vendors, and agencies, and allows for multiple organizations to participate in a channel.

e. Calls and Screen Sharing: Slack offers the ability to make calls and share work screens directly from channels and messages in the greater Slack platform.

10. Slack also claims that it synchronizes a particular user's tools in one seamless interface. This not only includes the integration of third-party applications like Google Drive, but also features the syncing of a user's activity across multiple devices and platforms. This means that, in addition to storing content of messages and activity across Slack platforms, the application captures device data connected to individual users. Such data may include attribution data for Slack users.

11. Therefore, the computers and/or servers of Slack are likely to contain stored electronic communications (including retrieved and unretrieved messages for Slack subscribers) and information concerning subscribers and their use of Slack services, such as account access information, message transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

12. In my training and experience, communications providers generally ask their subscribers to provide certain personal identifying information when registering for an account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

13. In my training and experience, communications providers typically retain certain transactional information about the creation and use of each account on their systems. This

information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, communications providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

14. As explained herein, information stored in connection with a Slack account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an electronic communications account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, messages, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, stored electronic data may provide relevant insight into the account user's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the users' motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

FACTS ESTABLISHING PROBABLE CAUSE

15. In 2018, Trevor Sumner (DOB: xx/xx/1984) and Kristopher Sipe (DOB: xx/xx/1974) co-founded Sun Badger Solar LLC, d/b/a Sun Badger Solar ("SBS"), in Wisconsin.

16. SBS provided residential and commercial solar installation services to homes and businesses in Wisconsin, Illinois, and Minnesota. SBS endorsed its solar systems as an alternative to save electricity and became one of the fastest growing solar companies in the Midwest.

17. Sumner and Sipe oversaw and directed SBS operations. Jointly, they controlled the practices of SBS.

18. SBS was also comprised of sales representatives and installation technicians. Sales representatives interacted directly with clients and promoted the benefits of SBS's solar systems. Under the direction of Sumner and Sipe, sales representatives composed contracts and discussed financial plans with clients. Installation technicians traveled to clients' homes and businesses to install solar systems. With the assistance of drafted system designs, installation technicians installed solar systems within contractual timeframes.

19. In 2022, Wisconsin, Illinois, and Minnesota government and law enforcement agencies noted an increase in consumer complaints regarding SBS. Specifically, several SBS customers complained to local law enforcement agencies, the Better Business Bureau, and the Consumer Protection Agency that SBS had taken some amount of payment from them but did not fulfill their contracts; instead, SBS abandoned solar installation projects, leaving the customers with unfinished work.

20. Despite SBS's struggle to manage its existing contracts, it appears that SBS continued to sign solar installation contracts with new clients. It also appears SBS did not advise new clients of its ongoing business struggles.

21. Local law enforcement officials interviewed dozens of SBS customers from January 2023 to May 2023. The customers generally reported that during contract negotiations, sales representatives offered clients an expedited installation timeline in exchange for cash deposits upon contact execution. Specifically, more than thirty-five clients reported that from April 2022 to December 2022, they paid a 50% cash deposit in exchange for the promise of receiving an installed solar system within timeframes as short as four months. To date, those clients have not received a fully installed solar system or financial refund. This is contrary to the Sun Badger Solar Sales Handbook, which states that "customers should never be promised something that we cannot guarantee. Install dates can never be guaranteed unless otherwise authorized by Kris, Ben, or Trevor."

22. In April 2023, the Minnesota Office of Attorney General interviewed Benjamin Gange, SBS's former national sales director and chief revenue officer. Gange advised that around March 2022, upper management instructed SBS sales representatives to continue to promise clients shortened timeframes for project installation, even though the timeframes could not and would not be met. Some sales representatives resisted, knowing the promised installation timeline was false and fraudulent; however, many sales representatives felt obligated to obey their supervisor and therefore conveyed to customers, in order to induce the customer to sign a contract with SBS and pay a cash deposit, "guaranteed" installation dates that the SBS sales representatives knew could not be met.

23. In Fall 2022, SBS hired a third party to conduct an internal financial audit. The results of the audit demonstrated that SBS was going through a financial crisis. Sumner and Sipe were aware of the audit's findings.

24. On or about December 16, 2022, Sumner sent an all-employee email advising staff of employee layoffs due to business restructuring. In the email, Sumner stated, "As you know the company is currently restructuring and rightsizing to plan for the future. As a result, there has been a need for a reduction in the organization's workforce. Yesterday several of our team members received layoff notifications. Those layoffs are now complete."

25. Despite this downsizing, SBS principals continued to direct sales representatives to promise clients solar installation dates that the principals knew were not achievable. In a declaration executed in Hennepin County, Minnesota, SBS's Minnesota Branch Manager, Kevin Armel Martin, stated that SBS did not have the installation technicians nor the products to service its existing clients, let alone new clients.

26. On or about January 13, 2023, SBS sent an email to its clients advising of installation timeframe delays. Sumner and Sipe co-authored the email, stating: "Over the past year, we've experienced unprecedented demand in the solar industry. That had been true not just at Sun Badger but across the country…We've come to realize that we overestimated our ability to fulfill some of our commitments in a timeframe that meets our standards…Sun Badger is not immune to the market stresses that all businesses are facing— price increases, work-force issues, and rising interest rates."

27. In March 2023, SBS terminated its LLC license leaving dozens of SBS clients with incomplete installation projects and abandoned contracts. According to a report generated by the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP), the total amount lost is approximately $1.3 million.

28. As part of its investigation into SBS's trade practices, the Office of the Minnesota Attorney General ("AG") interviewed former SBS employees, including former employee Cody

Pech. Mr. Pech provided to the Minnesota AG's office electronic of copies of messages that were created and exchanged by SBS employees on the SBS Slack account. For example:

a. A Slack message from Armel Martin, sent to a Slack channel among Minnesota staff, discusses a particular customer's project, which was long delayed and ultimately cancelled, as well as the Minnesota AG's investigation. In the message, Martin indicates that, "Today in our Ops manager meeting Kris was chuckling about and downplayed the situation. . . ."

b. Messages exchanged on a Slack channel titled "sales-bulletin-board" between Liam O'Donoghue and Nick Landauer about payment terms being offered to SBS customers.

29. These messages demonstrate that SBS employees used Slack to communicate and exchange information about the business, including about payment terms being offered to customers, installation timelines and delays, and an ongoing investigation into the business's trade practices. Your affiant believes that other Slack communications could similarly reveal information about false representations being made to customers in order to induce the customers to sign contacts with SBS and pay cash deposits, and the employees' and principals' knowledge of the falsity of those representations.

30. On August 15, 2023, FBI investigators sent preservation requests to Slack for Slack accounts associated with sunbadger.com, including but not limited to Debra Mahoney (SBS's Chief Financial Officer), Kristopher Sipe (SBS's Chief Operations Officer and co-founder), Trevor Sumner (SBS's President and co-founder), Benjamin Gange (SBS's Chief Revenue Officer), Nick Landauer (SBS's Vice President of Sales), Armel Martin (SBS' Minnesota Branch Manager),

kris@sunbadger.com, nick@sunbadger.com, trevor@sunbadger.com, for the time period January 1, 2021 to August 14, 2023.

CONCLUSION

31. Based on the above information, your affiant believes that there is probable cause to believe that SBS violated 18 U.S.C. § 1341 and 1343. Your affiant further believes that evidence of SBS's scheme will be retained and/or be within the possession, custody, or control of Slack. Your affiant further believes information retained by Slack, associated with SBS, will lead to evidence, fruits, and instrumentalities of the aforementioned crimes as well as to the identification of individuals who are engaged in the commission of those and related crimes.

32. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the services or execution of this warrant. The government will execute this warrant by serving the warrant via FedEx to Slack's headquarters. The warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to all information associated with the account identified as follows (the "SUBJECT ACCOUNT") that is within the possession, custody, or control of **Slack Technologies**, a company that accepts legal process at 500 Howard Street, California 94105, regardless of where such information is stored, held, or maintained:

- Sunbadger.com

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Slack Technologies (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on August 15, 2023, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

1. The contents of all communications associated with the account from January 1, 2021 to August 14, 2023, including stored or preserved copies of communications sent to and from the account, draft communications, the sender and recipient associated with each communication, the date and time at which each communication was sent, and the size and length of each communication;

2. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

3. The types of service utilized;

4. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

5. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within **fourteen (14) days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of 18 U.S.C. §§ 1341 and 1343, those violations involving Sun Badger Solar, Kristopher Sipe ("Sipe"), and Trevor Sumner ("Sumner"), and occurring after January 1, 2021, including but not limited to the following:

(a) Communications between Sumner, Sipe, Debra Mahoney, Kevin Armel Martin, Nick Landauer, Benjamin Ganje, and other Sun Badger Solar employees regarding payment terms for customers, cash deposits, installation timelines and delays, and ongoing investigations into the business's trade practices.

(b) Records that reveal the state of mind of Sun Badger Solar employees and principals with respect to the accuracy or falsity of representations being made to customers and other aspects of the crimes under investigation.

(c) Evidence indicating how and when the account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the account owner;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to signing solar panel contracts, upper-management meetings, employee trainings, or the company's financial condition, including records that help reveal their state of mind and whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits,

and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.