MillerMendel

1425 Broadway #430
Seattle, WA 98122
(206) 330-2094

Tyler Miller, President
(206) 333-4322

tjm@MillerMendel.com

Re: Serious Public Issues; Guardian Alliance Technologies ("Guardian") System

To Whom It May Concern:

I am the Founder, President and Chief Executive Officer of Miller Mendel, Inc. ("MMI"). MMI was founded in 2009 in Washington and pioneered the law enforcement background investigation software industry by creating the eSOPH background system for public safety agencies. Today, eSOPH is used by over 100 public safety agencies, including some of the largest (and smallest) agencies across the nation.

I care deeply about the law enforcement profession and the dedicated men and women of public safety agencies across the nation. I write now to address a serious public issue concerning your agency that impacts a large number of people. I understand that your agency is using the Guardian Alliance Technologies ("Guardian") background system. For both legal and ethical reasons, I am compelled to bring to your attention the potentially serious legal ramifications of using the Guardian system. If you take the time to read this entire letter, I am confident you will see why I am so concerned. **I strongly recommend you have your agency's legal counsel review this letter and the Attachments, without delay. The liability and legal implications to your agency and individual employees are significant.** This letter comes after review of Guardian's contract terms and conditions, Guardian's privacy policy, Guardian's marketing releases and marketing video(s). I encourage you to review these Guardian items and believe you will come to the same opinion I have reached.

This letter addresses two important topics of public concern: 1) legal compliance and ethical dilemmas related to agency, applicants and applicants' references use of the Guardian system impacting privacy rights and misuse of applicant's private information; and 2) grounds for continued patent infringement lawsuits against agencies using the Guardian system.

In summary: Guardian's contract between Guardian and the agency gives Guardian control and data sharing permission over highly sensitive and confidential data that your agency, applicants and applicants' references enter into the Guardian system. The Guardian contract appears to permit Guardian to commercialize your applicants' sensitive personal information, share your agency's narrative/summary report(s) regarding the investigation into the applicant, and contains no provision to keep references' responses or references' identities confidential. As such, it appears that using Guardian prevents your agency from complying with confidentiality, privacy and data security regulations and your agency's legal and ethical obligations to applicants and applicants' references who are compelled to provide information during the background investigation process.

It's well established across the nation that agencies must not disclose background information submitted in confidence if the provider requests confidentiality, confidentiality was represented, or where required or allowed by law, as there is a strong public interest in obtaining complete and accurate background information on an applicant to a position in public trust. Disclosure of confidential background information can harm public interest by making providers of background information reluctant to share relevant information, and thus may enable the hiring of personnel who may have significant background issues that would have been excluded from employment had the information been known by the hiring agency.

Agency Legal Compliance and Ethical Concerns

If your agency is using the Guardian system under Guardian's "Terms of Service for the Guardian Platform" and "Guardian's Privacy Policy" agreements (linked below), **I strongly recommend you have your legal counsel review this letter and the Attachments, without delay. The liability and legal implications are significant.**

I recently received copies of Guardian's Terms of Service for the Guardian Platform and Privacy Policy (Attachment 4), as well as the "Platform Activation Agreement" (Attachment 7) in response to a public records request to the Gilbert Arizona Police Department. The records the city provided are extremely concerning. Your agency and employees should be fully informed of the implications certain terms cause your agency, your employees, applicants and applicants' references. Multiple agencies, after engaging their legal counsel for an independent legal review, have discontinued use of the Guardian system.

I believe if you review the Guardian contracts, you will have the opinion that they obligate your agency and your agency's employees to the Guardian Terms of Use and Guardian Privacy Policy if you so much as use the system, whether you signed something or not (see Attachment 4, Page 18).

1. **Unlawful Indemnification.** The Terms of Service for the Guardian Platform require your agency and your employees using the system to indemnify Guardian in claims related to your agency's use of the Guardian system (see Attachment 4, Section 10 (g))--

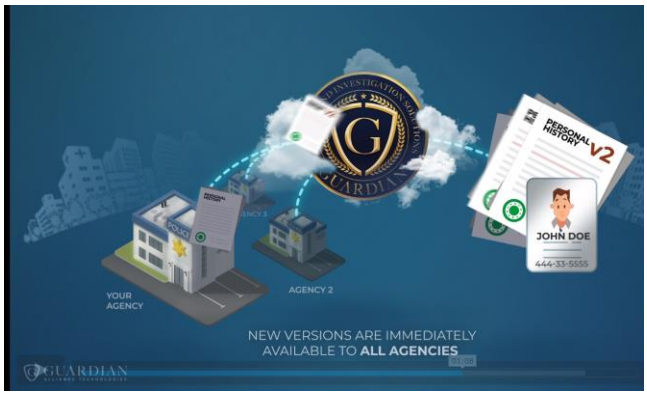
   > **g. Indemnity.** Each respective User agrees to defend, indemnify, and hold harmless Guardian (and its subsidiaries, affiliates, officers, directors, employees and agents) from and against any third-party claims, actions or demands (including, without limitation, costs, damages and reasonable legal and accounting fees) alleging or resulting from or in connection with their use of the Platform, any Document posted by them, their use of the Platform or their breach of this Agreement.

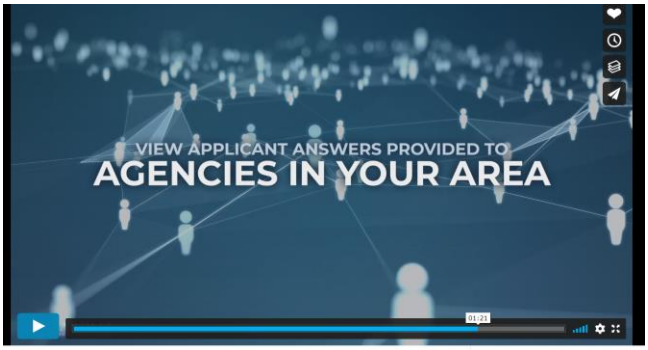
   It is unlawful in several states (e.g., Colorado) for a public agency to indemnify a private company. Through this term, your agency and your employees (including contractors) logging into the Guardian system **are agreeing to personally indemnify Guardian.**

Moreover, the contract does not apply a maximum amount ("limit cap") to the indemnification.

2. **Applicants' Personal Information.** Please review the Guardian contract terms as they relate to Applicant's personal information. We believe you will come to the opinion that under the Guardian contract terms, you grant Guardian permission to share a wide range of data the system collects about your applicants with other agencies, contractors, and commercial affiliates (see Attachment 4, Pages 20 and 21).

   One of Guardian's marketing videos explains a sharing functionality of the Guardian system: https://vimeo.com/465149470 (pay especially close attention to what's explained starting at 0:50 seconds into the video: "the applicant's certified personal history information is released to connected agencies")--





Guardian's marketing video describes creating a private national database of applicants to public safety agencies using the Guardian Platform, "National Applicant Information Center" ("NAIC"). This platform shares the applicants' data with other agencies. The video states that an agency may "View applicant answers provided to agencies in your area," that agency investigators have the ability to see any answer given by an applicant to any agency using the Guardian Platform, and that the NAIC is a data warehouse of the applicants' personal information which is shared downstream with third party Guardian clients. The video states that if the applicant's answers differ from an answer given in application submitted to your agency, the Guardian system "immediately" notifies the **third party** Guardian client(s) and discloses the conflicting answer the applicant gave to your

agency to their third party clients. Guardian also stated in a press release and on its website that it has opened the Guardian software and NAIC database to private investigation firms/private investigators who are not employees of public safety/government agencies.

Despite the sharing activity of the Guardian system the marketing video depicts and the Guardian Terms of Use and Guardian Privacy Policy, on April 16, 2021, Guardian's Chief Operating Officer represented to the Goodyear Police Department: "At no time does Guardian share applicant data with anyone…." (See Attachment 5). We believe that is a concerning statement in light of the marketing video and Guardian's own contract terms.

Further considerations related to Attachment 4, Page 20 and 21; Information you authorize Guardian to share:

- Are you using Guardian's reference system where the applicants' references are asked questions about the applicant? Are you representing to those references their responses to those questions are confidential or privileged under the law? If so, I have the opinion that you may be making a false promise to the reference. Based on Guardian's Terms of Use and Privacy Policy, Guardian can share the information references provide as noted above.

  California law (and perhaps other states) says that providers of information during a legally mandated background investigation have absolute privilege. See, for example, California Information Practices Act 11, the Investigative Consumer Reporting Agencies Act 12, Civil Code §47, §1786 et seq, §1798, Johnson v. Winter 127 Cal App. 3d 435, McQuirk v. Donnelly, 189 F.3d 793 (USCA 9th 1999).

  I have the opinion that a review of Guardian's Terms of Use and Privacy Policy establishes that if your agency promises references confidentiality or represents that the reference will receive confidentiality under the law or department policy, your agency should not use the Guardian system to save information that identifies the reference or identify the reference in the investigator's narrative summary/report(s) because Guardian's Privacy Policy authorizes Guardian to share your narrative report and other information on the Guardian system.

- Data received from credit reports, TLO, Accurint, and similar sources then uploaded to Guardian or referenced in a document uploaded to Guardian may cause your agency to breach your agreement term(s) with those providers or violate applicable laws, like the federal Fair Credit Reporting Act. Some states also have laws governing the use of and access to credit data.

- Permitting a private company to use (or share) information collected to complete a legally required background investigation related to a government entity is

incompatible with the spirit of the law that allowed your agency to require the information from the applicant (and potentially applicant’s references).

- There may be additional laws in your state the Guardian Terms of Use and Guardian Privacy Policy are not compatible with due to the way Guardian shares personal data related to a background investigation of an applicant to a public entity.

3. **Guardian Is Authorized to Share Data From Your Background Investigation; You Are Responsible.** It is MMI’s opinion that Guardian’s Terms of Use and Privacy Policy authorizes Guardian to share applicant data with other Guardian users, so your applicants’ data adds value to the services Guardian offers other agencies and commercial affiliates. But the contract also makes your agency and your employees legally responsible for the accuracy of data they input to the Guardian system (see Attachment 4, Section 11 (c)). Keep in mind your agency and your employees and contractors also agree to indemnify Guardian against third-party claims related to their use of the Guardian system. Guardian also denies any responsibility for information posted or uploaded to the Guardian system and states it “has no obligation to screen communications or information in advance” or screen or monitor postings by other users (see Attachment 4, Section 16 (a)).

4. **Guardian Contract Terms Do Not Limit How Third Parties Access or Use The Data You Or Your Applicants Enter.** Per the Guardian contract terms, Guardian can permit their other clients and commercial affiliates to download your applicants’ personal information for their own purposes and maintain that sensitive, confidential data on their own IT systems. Those other clients and commercial affiliates are permitted to contact your applicants directly, and to use, process, and store your applicants’ sensitive, confidential data as they wish without any monitoring or limitations from Guardian (see Attachment 4, Page 21).

   Applicants input their personal information to the Guardian system to be considered for employment with your agency because you asked or required them to do so. Using software that permits unvetted and unmonitored third parties to access and process applicant data is likely to increase your agency’s legal risk.

   - **Authorized Access to Data:** How can your agency confirm that third parties using the Guardian system are vetted and cleared to access the confidential or private data? How does that impact CJIS compliance and other compliance regimes your agency may be subject to through laws specific to your state or jurisdiction?

   - **Data Breach:** How would your agency know if the data your agency caused to be entered into the Guardian system is impacted by a data breach on the third party’s IT system? Without knowing this, how can your agency comply with data breach notification laws applicable in your state or jurisdiction?

- **Public Records Laws:** How can your agency assert exemptions to public records/FOIA requests if Guardian has already released the same or similar data, and through that practice, established the information is not private or exempt? Your agency may be waiving public records law exemption assertions it could have made had the information been owned and controlled by your entity; the Guardian terms establish Guardian (a private, for-profit company) has first level control over data about the applicant and information you and applicants’ references added into the Guardian system.

- **Records Retention And Destruction:** How do you comply with your state’s public records retention and destruction laws with respect to data stored on an unknown third party’s database and a private company’s IT system?

- **Protection Of Your Employees’ Data And Their Privacy:** How can your agency safeguard law enforcement officers’ sensitive personal information from unlawful or unauthorized disclosure? Will your officers’ union take issue with the way their members’ private data is stored and potentially shared? How do you protect lateral employees’ requests for temporary confidentiality or privacy when they apply to a different agency?

- **Discovery Issues:** If an applicant files a lawsuit, how do you control discovery requests when your agency cannot assert first level control over the data? What information gets released from applicant investigation files to use in that lawsuit, creating privacy issues for uninvolved applicants and agencies? What if the lawsuit takes place in a different state where civil procedure, to include discovery, is different from your jurisdiction?

5. **No User Authentication.** “Guardian cannot and does not confirm that each user is who they claim to be.” Moreover, Guardian requires your agency to release it from any disputes among users (Attachment 4, Section 10 (e)). Put simply, Guardian can allow third parties to access and use your agency’s data but has no contractual obligation to you to ensure that data is only accessible to authorized users and will not assist with any issues between your agency and other users. Guardian contract terms are silent as to any effort to log or track how data is dispersed. Based on these documents, it is unclear how Guardian practices comply with CJIS security policy.

6. **Guardian’s Terms of Use and Privacy Policy Do Not Support Privacy Law Compliance.** Guardian’s Terms of Use and Privacy Policy require your agency’s individual employees and applicants to use the Guardian system in compliance with applicable privacy and data processing laws (Attachment 4, Section 11 (c)). However, Guardian appears to engage in data sharing activities that conflict with those laws by not providing a system that offers adequate notice or opt-outs of that sharing. Keep in mind

your agency and its end users also agree to indemnify Guardian against third party claims related to their use of the Guardian system.

7. **No Promise of Privacy Practices.** Under the Platform Activation Agreement, your agency and Guardian each agree to maintain a legally compliant security program (Attachment 7, Section 3.8). However, Guardian does not contractually agree to comply with privacy laws or regulations and reserves the right to disclose applicant personal information in violation of Guardian’s own Privacy Policy “to comply, at [Guardian’s] sole discretion, with legal requirements…” (Attachment 4, Section 11(a)). In sum, Guardian does not offer agencies any reliable privacy practices to ensure applicants and other end users.

8. **Refusal to Delete Data.** According to the Privacy Policy, Guardian does not delete an applicant’s personal information or any of your agency’s data, ever (Attachment 4, Page 22). Lengthy or, in this case, perpetual data retention by vendors will prevent your agency from meeting any applicable data security standards and significantly increases your agency’s risk if a data breach occurs. Many state laws require you to delete or update a user’s personal information upon request. Guardian’s policy to never delete data means Guardian is noncompliant with applicable laws and your agency cannot purport to comply with laws or regulations requiring data deletion or correction.

9. **No Mention of Insurance.** The Guardian agreements are silent as to whether Guardian has or will maintain insurance to cover your agency in the event of a data breach or other event that causes your agency to incur liability or costs. It is common for city, county, or state contract procurement laws or regulations to require vendors to carry appropriate general liability, errors and emissions, and/or cyber insurance in amounts appropriate to help your agency recover costs incurred due to the vendor’s negligence or tortious act.

10. **California Courts. California Law.** Guardian contracts require that any legal actions brought between your agency, your employees, applicants and Guardian relating to Guardian services are subject to California law and must be filed and litigated in California courts. In MMI’s experience, public agencies cannot agree to governing law or a venue outside of the agency’s home state.

As you can see from the outline above, you are granting Guardian permission to collect data and put data to use per Guardian’s discretion, outside of your agency’s control.

Applicants to law enforcement careers must provide very private information about their life history, much of which is required by law or government agency policy. In contrast, a private sector employer requiring the same information of an applicant would be in violation of employment laws. For this reason, it is imperative that your agency maintain first level control over applicants’ data, data applicants’ references provide and the data your agency’s employees save to the Guardian system.

Patent Infringement

In or around 2016, Guardian surfaced offering a competing software to MMI's eSOPH system. Shortly thereafter, MMI learned use of Guardian's competing system likely infringed MMI's U.S. Patent No. 10043188.

The law concerning patents is very clear; patents issued by the United States Patent and Trademark Office ("USPTO") are valid and the only authority that can invalidate ("revoke") a patent is the USPTO or a federal court. Additionally, **end users** are liable for using the infringing software. Since discovering the patent infringement, MMI has filed several patent infringement lawsuits in federal district courts against the law enforcement agencies using the Guardian software. MMI intends to continue filing lawsuits to protect MMI's clients, MMI's intellectual property and MMI's business interests.

MMI has been asked why it has filed lawsuits against agencies using the Guardian software. The answer is this: the actual use of the Guardian software by the agency is the damaging aspect to MMI. If Guardian made the software but no agency "bought" the software to use, monetary damage would be little. The agency paying Guardian to use the infringing software is where the damage begins and continues. Filing a federal lawsuit against the agency also may ensure MMI is able to recover damages in the event Guardian were to file for bankruptcy, especially in the event Guardian lacks applicable insurance coverage. To be clear, MMI has not filed lawsuits against agencies who were unaware of the patent; MMI has advised the defendant agencies of the patent, asked them to cease infringement, and only when they did not cease infringement did MMI file a federal lawsuit against the agency. At that point, MMI contends the agency is deciding to **willfully** infringe a valid USPTO-issued patent.

The legal process to date overwhelming favors MMI's belief that Guardian infringes MMI's patent.

- An expert technical witness inspected the Guardian system and opined that the Guardian system was **clearly infringing** on MMI's patent. The expert witness stated, "it was like Guardian read the patent to design their system."

- In 2020, legal counsel for Guardian filed a petition for an "Inter Partes Review" ("IPR") with the USPTO, asserting the MMI's 10043188 patent covering certain features and functionality of the eSOPH system is invalid. The USPTO **rejected** Guardian's IPR petition and highlighted Guardian's significant misunderstanding of patents and the IPR process (see Attachment 1).

- Guardian appealed the USPTO's decision and, in response, the USPTO issued another decision **denying Guardian's appeal** (see Attachment 2).

- Guardian then filed a request for a USPTO Procedural Opinion Panel, which was also denied (see Attachment 3).

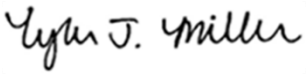
The USPTO IPR filings by Guardian were reviewed and decided by a panel of three qualified USPTO judges. There is no better authority to understand and rule on patent-related disputes than attorneys who have practiced in the specific area of law. The written opinions of the USPTO judges and the Procedural Opinion Panel (Attachments 1 through 3, linked above) offer clear insight into Guardian’s desperate and failed attempts to invalidate MMI’s patent.

Put simply, if your agency is using the Guardian system, it is MMI’s opinion that your agency and employees are **willfully infringing** MMI’s intellectual property and may be subject to a patent infringement lawsuit and perhaps additional claims. If a government entity uses another’s property, the agency may be subject to a state and/or federal law taking claim. Regardless of whether Guardian indemnifies your agency and employees for your use of the Guardian software, your agency and employees will have to navigate the complicated process of defending yourselves in a patent infringement lawsuit, which includes producing labor-intensive discovery and (potentially) appearing for depositions.

Patents are property of the owner. If you use infringing software, your agency is depriving someone of “Just Compensation” for use of their property rights. Just as you would not make a false arrest, you should not deprive someone of their property rights. The taking of intellectual property is no different. It’s also important to understand such conduct is not compatible with the oath of office law enforcement officers take, nor is it compatible with most states’ ethics laws that apply to public officials.

My statements above (and in my previous communications) are my opinions based on my observations, understanding of rules and regulations and discussions with legal counsel. Your city’s administrative and legal personnel should independently review these topics and make their decisions based on their own independent reviews.

Sincerely,



Tyler Miller
President & CEO

Attachments: Attachments are linked in-line where they are referenced and also attached as pages hereto. If a link to an Attachment does not work, please contact MMI at (206) 333-4322 or email tjm@MillerMendel.com

GUARDIAN ALLIANCE TECHNOLOGIES, INC.

TERMS OF SERVICE FOR THE GUARDIAN PLATFORM
Last Revised: January 5, 2021

1. INTRODUCTION

The following terms and conditions (the "Terms") govern all access to the cloud-based software platform owned by Guardian Alliance Technologies, Inc. as well as the access and use of any Integrated Services as defined herein (collectively the "Platform"). Guardian Alliance Technologies, Inc. is referred to herein as "Guardian".

The Platform is offered subject to your acceptance, without modification, of all of the terms and conditions contained herein and all other operating rules, policies and procedures that may be published from time to time on the Platform, including, without limitation, Guardian's Privacy Policy. If you do not accept these Terms or you do not meet or comply with their provisions, you may not use the Platform.

If your use of the Platform is the result of having entered into a separate, manually or digitally-executed agreement ("Separate Agreement"), the terms and conditions of the Separate Agreement(s) are automatically part of this agreement and if any of the terms and conditions of any such Separate Agreement contradicts any of the provisions of these Terms, including the pricing of OnDemand Features and associated Invoicing and Payment Terms as outlined in Section 4 herein, the terms and conditions of the Separate Agreement shall prevail.

2. INTEGRATED SERVICES

Guardian has contracted with third party technology service providers in an effort to provide robust Service offerings to Customers through integrated utilities within the Platform. In the event that Customer uses any of these Integrated Services, Customer is bound by the terms and conditions of those Integrated Service Providers. Current Integrated Services include:

a. **Social Media Screening Services.** Guardian is an authorized Reseller of social media screening services (the "Social Media Screenings"), which is provided to Customers through the use of a technology platform developed, owned and operated by Fama Technologies, Inc ("Fama"), a Delaware corporation located at, 5340 Alla Rd, Suite 104, Los Angeles, CA 90034. Customers may use the Social Media Screening Services directly through the Platform subject to Fama's User Terms and Conditions and other Terms and Conditions outlined herein. Fama is a third party beneficiary to these Terms.

3. FREE VS ON-DEMAND FEATURES

All Applicant facing features of the Platform are available for use by Applicants free of charge and some features of the Platform are available for use by Customers at no cost. Other features of the Platform are available for use by Customers, on an OnDemand basis, in exchange for a fee as

outlined in Section 4 herein. The OnDemand Features of the Platform can only be authorized for use by the Customer's Account Administrator, as defined herein. If these features are not authorized for use under your account, they may be inaccessible to you. If you are unsure of whether you are authorized to use the OnDemand Features, please consult with your Account Administrator. Current OnDemand Features are:

a. Investigation Processing Services; and

b. Social Media Screening Services; and

c. Credit Report Services.

4. FEES, INVOICING, AND PAYMENT FOR SERVICES

In the event that the Account Administrator activates OnDemand features for use by Authorized Users, the following Fees, Invoicing and Payment policies shall apply:

a. Background Investigations. Customer understands that a Fee of $50 will be incurred each time an investigation is assigned to an Investigator. Customer agrees to pay any/all such fees in accordance with the payment terms set forth in the Platform Activation Agreement. No Fee is incurred by the Applicant.

b. Social Media Screenings. In exchange for use of the Platform for the purposes of conducting a Social Media Screening on Applicants or Employees, Customer understands that a Fee of $40 will be incurred each time a Social Media Screening Report is ordered. Customer agrees to pay any/all such fees in accordance with the payment terms set forth in the Platform Activation Agreement. No Fee is incurred by the Applicant or Employee.

c. Credit Report Services. In exchange for use of the Platform for the purposes of ordering Credit Reports on Applicants or Employees, Customer understands that a Fee of $12 will be incurred each time a Credit Report is ordered. Customer agrees to pay any/all such fees in accordance with the payment terms set forth in the Platform Activation Agreement. No Fee is incurred by the Applicant or Employee.

d. Invoicing. Invoices for use of the Services shall be issued at the beginning of each calendar month for all use of Fee Based Features occurring through Customer's account during the preceding calendar month.

e. Payments. Customer shall pay all sums due under this Agreement within 30 days of receipt of invoice.

f. Failure to Pay/Customer Conduct. Guardian reserves the right to suspend or terminate access to the Services if any payment is delinquent by more than thirty (30) days.

5. USER LICENSE

Subject to the terms and conditions contained herein, Guardian hereby grants you a limited, terminable, non-exclusive right right (a "User License") to access and/or use the Platform. Users assume all responsibility and risk for their accessing and/or using the Platform, the Internet

generally, and the Documents that Users use, post, provide, collect or access and for their respective conduct on and off the Platform.

a. **Applicants.** Your User License is exclusively for your personal access to and use of the Platform. Applicants hereby agree that they are solely responsible for the content of any Document(s) or information posted to or collected through the Platform and for any consequences arising from such posting.

b. **Employees.** Your User License is exclusively for your personal access to and use of the Platform. Employees hereby agree that they are solely responsible for the content of any Document(s) or information posted to or collected through the Platform and for any consequences arising from such posting.

c. **Employers.** Your User License provides your authorized Employer representatives, agents, contractors, affiliates, and/or employees with the right to access and use the Platform for the purpose of collecting, organizing, reviewing and evaluating Documents and other information related to Applicants and Employees in the process of considering and/or re-verifying (in the case of Employees) qualifications and eligibility for employment.

d. **Third Party Agents for Applicants or Employers.** Your User License provides your authorized representatives, agents, contractors, affiliates, and/or employees with the right to access and use the Platform for the purpose of collecting, organizing, reviewing and evaluating Documents and other information related to Applicants in process of considering qualifications and eligibility for introductions to potential Employers.

6. BINDING AGREEMENT

These Terms are a binding agreement between you and Guardian Alliance Technologies, Inc. By accessing or using any part of the Platform, you agree to become bound by the terms and conditions of this Agreement.

7. AMENDMENTS TO THIS AGREEMENT AND CHANGES TO THE PLATFORM.

Guardian may revise these Terms, and/or Privacy Policy at any time, at Guardian's sole discretion. If/when updated, the updated Terms and/or Privacy Policy will be made known to Users and changes will be binding on Users on the date they are posted on the Platform (or as otherwise stated in any notice of such changes). Any User access of, or use of, the Platform will be considered User acceptance of the then-updated Terms and/or Privacy Policy (including any exhibits thereto) as published. If, at any time, a User deems the Terms and/or Privacy Policy unacceptable, such User may not use the Platform any longer. Any new or different terms supplied by Users are specifically rejected by Guardian unless Guardian agrees to them in a Separate Agreement. Guardian may change the Platform at any time.

8. LEGAL AUTHORITY

If you are entering into this Agreement on behalf of a corporation, municipality or government entity, you represent and warrant that you have the legal authority to bind such entity to the terms and conditions contained in this Agreement. Guardian shall not be liable for any loss or damage resulting from Guardian's reliance on any instruction, notice, document or communication reasonably believed by Guardian to be genuine and originating from an authorized representative of your entity. If there is reasonable doubt about the authenticity of any such instruction, notice, document or communication, Guardian reserves the right (but undertakes no duty) to require additional authentication from you. You further agree to be bound by the terms of this Agreement for transactions entered into by you, anyone acting as your agent and anyone who uses your account to access or use the Platform, whether or not authorized by you.

9. DEFINITIONS

a. **"Account Administrator",** also known as a "Supervisor User" on the Platform means an individual User, chosen by an Employer, who is responsible for managing all activity occurring under the Employer's Account, including the activation and/or deactivation of Authorized User accounts for Employer personnel who are authorized to access and use the Platform on behalf of the Employer.

b. **"Aggregate Data"** means de-identified or anonymized data or information, including, by way of example and not limitation, information or data relating to occupation, location, salary, education, experience, zip code, age, gender, race or ethnicity of many individuals that is combined together.

c. **"Applicant"** means an individual who creates a User Account for the purposes of submitting their Documents and other information to the Platform for review, evaluation, and consideration by Employers in the process of seeking employment with an Employer. Applicants incur no fees associated with their use of the Platform.

d. **"Content"** means material delivered or presented on the Platform, including but not limited to web pages, web forms, programming (including software code used on the Platform, including (i) tools, kits, and object libraries, (ii) all third-party or open source code embedded therein, and (iii) any upgrades, updates, releases, fixes, enhancements or modifications to the foregoing), graphics, images, design (color combinations and page layout), text, information, data, resumes stored in various commercial databases operated and licensed by Guardian, data submitted via the Platform by Users and other content made available on or through the Platform by Guardian.

e. **"Credit Report"** means a detailed breakdown of an applicant credit history prepared by a credit bureau.

f. **"Customer"** refers to any Employer who is paying a fee for access to and/or use of the Platform.

g. **"Document"** refers to any posting to the Platform, including, without limitation, resumes, waivers, profiles, birth certificates, etc.

h. **"Employer"** means a corporation, municipality or government entity, represented by an individual to establish an Employer Account on its behalf and which is accessing the Platform to collect, organize, review and evaluate Documents and/or other Applicant information or to use the Platform for any reason related to the purposes for which the Platform is designed.

i. **"Employer Account"** means an account established for an Employer for the purpose of accessing and using the Platform through one or more User Accounts. Employer Accounts are managed by the Employer's Account Administrator.

j. **"Fee Based Features"** means the Assignment For Investigation Processing and the Social Media Screening features of the Platform.

k. **"Guardian Materials"** includes any materials, methodologies, implementation plans, or other intellectual property used during the provision of Services.

l. **"Integrated Services"** means any services provided by a third party technology provider accessible through the Platform.

m. **"Investigator"** means an Authorized User on the Platform who is eligible and authorized by a party other than Guardian to conduct a pre-employment background investigation of an Applicant.

n. **"Assignment"** means that an Account Administrator has Assigned an Applicant record to an Investigator for the commencement/continuance of a pre-employment investigation.

o. **"Integrated Service Provider"** means any third party technology service provider with whom Guardian has contracted for the purposes of offering their technology service as an Integrated Service accessible through the Platform.

p. **"Services"** means any services provided by Guardian or its agents through or related to the Platform.

q. **"Social Media Screening"** means the collection and analysis of all publicly available online information about an individual, including material gathered from Social Media accounts.

r. **"Third Party Agents"** means any third party service provider who is acting as an intermediary between Employers and Applicants in an effort to bring the two together.

s. **"User" or "Users"** refers to

   i. any Employer representatives, agents, contractors, affiliates, and/or employees who are authorized to use the Platform on behalf of Employer and who have User Accounts for access to and use of the Platform; and/or

   ii. Applicants or Employees who have created a User Account for the purposes of accessing and using the Platform.

   iii. Third Party Agents for Applicants and/or Employers who are authorized to use the Platform for the sole purpose of introducing Applicants to Employers.

t. **"User Account"** means an individual account consisting of a unique Username and Password combination, which is utilized exclusively by one person for purposes of accessing and using the Platform.

u. **"You" or "you"** means the person who is agreeing to these Terms by virtue of their access and use to and of the Platform.

10. USE OF THE PLATFORM AND SERVICES

a. **Lawful Use.** Users may use the Platform only for lawful purposes within the context of the Intended Platform Use.

b. **Intended Platform Use.** The Platform is intended for;

   i. use by individual Applicants or Employees to post Documents and other materials containing information for review by Employers; and

   ii. use by Employers to collect and manage Documents and other materials containing Applicant or Employee information for the purpose of reviewing, evaluating, and considering the Applicant's qualifications and eligibility for employment and for the purposes of updating the files of current Employees, as is periodically necessary pursuant to the internal policies for some Customers.

iii. use by Third Party Agents to collect and manage Documents and other materials containing Applicant information for the exclusive purpose of introducing Applicants and Employers to one another.

c. **User Accounts.** In order for you to access and use the Platform, You, an Account Administrator, or Guardian will be required to create a User Account for you consisting of a unique Username and password combination. If an account is established for you by an Account Administrator, your Account Administrator will be able to access and make changes to your account without your or our involvement.

d. **User Account Confidentiality.**

i. The Platform is to be accessed and used through User Accounts solely by the User to whom the account is registered. Users are prohibited from providing their password or otherwise permitting access to their Guardian account to any third party.

ii. Users are solely responsible for maintaining the confidentiality of their information and password.

iii. You hereby agree to protect and keep your password confidential and to change your password on a regular basis, consistent with Guardian requirements and/or the policies of your Employer.

iv. Users are responsible for all uses of their account, whether or not authorized by them. If others use your password to post inappropriate material on the Platform, the User to whom the account is registered risks losing their access to the Platform.

v. You hereby agree to notify Guardian and/or your Account Administrator immediately of any unauthorized use of your account or password.

e. **User Authentication**. Because User authentication on the Internet is difficult, Guardian cannot and does not confirm that each User is who they claim to be. Because Guardian does not and cannot be involved in User-to-User dealings or control the behavior of participants on the Platform, in the event that you have a dispute with one or more Users, you release Guardian from claims, demands and damages (actual and consequential and direct and indirect) of every kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed, arising out of or in any way connected with such disputes.

f. **User Network.** User acknowledges and agrees that:

i. User is responsible for selecting appropriate remediation for, and resolving, any issues found on their network or in User's web traffic through the use of the Platform; and

ii. Guardian is not liable for, or responsible to, remediate any issues found on User's network or in User's web traffic through the use of the Platform.

g. **Indemnity.** Each respective User agrees to defend, indemnify, and hold harmless Guardian (and its subsidiaries, affiliates, officers, directors, employees and agents) from and against any third party claims, actions or demands (including, without limitation, costs, damages and reasonable legal and accounting fees) alleging or resulting from or in connection with their use of the Platform, any Document posted by them, their use of the Platform or their breach of this Agreement. Guardian shall use reasonable efforts to provide Users with prompt notice of any such claim, suit, or proceeding and may assist User, at User's expense, in defending any such claim, suit or proceeding. This indemnification shall not extend to any loss, damage, injury, or costs to the extent caused by the negligence or willful misconduct of Guardian, or its employees.

11. USE OF INFORMATION

a. **User Information.** User Information will be used in accordance with the terms of Guardian's Privacy Policy. Please note, as set forth in the Guardian Privacy Policy, that Guardian may collect certain User Information and may contact Users periodically in accordance with the terms of the Guardian Privacy Policy. In addition, Guardian reserves the right to comply, in its sole discretion, with legal requirements, requests from law enforcement agencies or requests from government entities, even to the extent that such compliance may require disclosure of certain Information. In addition, third parties may retain cached copies of User Information.

b. **Use of Aggregate Data.** You understand and agree that Guardian owns and has the right to collect, extract, compile, synthesize, and analyze Aggregate Data as defined herein. Guardian may use such Aggregate Data for any lawful business purpose without a duty of accounting to any User, provided that the data and information is used only in an aggregated and anonymized form so that it cannot be identifiable as relating to you or to any other individual Applicant.

c. **Data Security, Accuracy, Completeness.** User represents and warrants that it is and will continue to be compliant with all applicable privacy and data protection laws and regulations with respect to any Applicant Data. User shall be solely responsible for the accuracy and completeness of all records, databases, data and information provided, submitted or uploaded in connection with use of the Platform.

d. **Electronic Communication and Notices.** When you use the Platform or send communications to us through the Platform, you are communicating with us electronically. You hereby consent to receive, electronically, any communications related to your use of the

Platform. We may communicate with you by email or by posting notices on the Platform. You agree that all agreements, notices, disclosures and other communications that are provided to you electronically satisfy any legal requirement that such communications be in writing. All notices from us intended for receipt by you shall be deemed delivered and effective when sent to the email address you provide to us. Please note that by submitting Content, creating a user account or otherwise providing us with your email address, postal address or phone number, you are agreeing that we or our agents may contact you at that address or number in a manner consistent with our Privacy Policy.

12. OWNERSHIP

a. Intellectual Property Rights. The Platform, the Guardian Materials and all right, title and interest in and to the Platform and Guardian Materials are the sole property of Guardian or its licensors, and are protected by United States and foreign copyright, trademark and other laws. Except for the limited licenses expressly granted to Users by these Terms, Guardian reserves for itself and its licensors all other rights, title and interest. Without limitation on the foregoing, Users may not reproduce, modify, display, sell, or distribute the Content or Guardian Materials, or use them in any other way for public or commercial purposes. Notwithstanding anything to the contrary contained herein, this prohibition includes:

i. copying or adapting the HTML code used to generate web pages on the Platform;

ii. using or attempting to use engines, manual or automated software, tools, devices, agents, scripts, robots or other means, devices, mechanisms or processes (including, but not limited to, browsers, spiders, robots, avatars or intelligent agents) to navigate, search, access, "scrape," "crawl," or "spider" any web pages or any Services provided on or through the Platform other than the search engine and search agents available from Guardian on the Platform, other than generally available third party web browsers (e.g., Internet Explorer, Firefox, Safari, etc); and

iii. aggregating, copying or duplicating in any manner any of the Content or information available from any of the Platform, without the express written consent of Guardian. The use of the Content on any other web Platform or in a networked computer environment for any purpose is strictly prohibited. The Guardian design logo and certain other names or logos are service marks or trademarks of Guardian, and all related product and service names, design marks and slogans are the service marks or trademarks of Guardian. In addition, the "look" and "feel" of the Platform (including color combinations, button shapes, layout, design and all other graphical elements) are also protected by Guardian's trademarks, service marks and/or copyrights. Any code that Guardian creates to generate or display the Content or the pages making up the Platform is also protected by Guardian's copyright. You must retain all copyright, trademark,

service mark and other proprietary notices contained on the Content or Guardian Materials on any authorized copy you make of the Content or Guardian Materials. All other product and service marks contained on the Platform are the trademarks of their respective owners.

b. User Submissions. Guardian welcomes User comments regarding the Platform. Please note, however, that Guardian does not accept or consider creative ideas, suggestions, inventions or materials other than those it has specifically requested. If, despite this notice, a User submits creative suggestions, ideas, drawings, concepts, inventions, or other information (a "User Submission"), the User agrees that such User Submission shall become the property of Guardian. User Submissions and any elements contained in User Submissions, shall not be subject to any obligation of confidentiality on Guardian's part, and Guardian will not be liable for any use or disclosure of any User Submission. Guardian shall exclusively own all now known or later discovered rights to the User Submission and shall be entitled to unrestricted use of the User Submission for any purpose whatsoever, commercial or otherwise, without compensation to you or any other person.

13. AVAILABILITY OF THE PLATFORM

a. Service Level Objectives. Subject to these Terms and our other policies and procedures, we shall use commercially reasonable efforts to attempt to ensure that the Platform is available for use twenty-four (24) hours a day, seven (7) days a week basis. You acknowledge and agree that, from time to time, the Platform may be inaccessible or inoperable for any reason including, but not limited to, equipment malfunctions; periodic maintenance, repairs or replacements that we undertake from time to time; or causes beyond our reasonable control or that are not reasonably foreseeable, including, but not limited to, interruption or failure of telecommunication or digital transmission links, hostile network attacks, network congestion or other failures. You acknowledge and agree that we have no control over the availability of this Platform on a continuous or uninterrupted basis, and that we assume no liability to you or any other party with regard thereto. The Platform will be considered unavailable only when there is no external connectivity for a five-minute period or longer and Customer is unable to launch replacement instances. Guardian will use commercially reasonable efforts to meet the following RTO (Recovery Time Objective) and RPO (Recovery Point Objective) targets of 20 hours and 4 hours respectively.

b. Scheduled Downtime. From time to time, Guardian will schedule system downtime ("Scheduled Downtime) to perform system maintenance, backup and upgrade functions for the Platform. During Scheduled Downtime, the Platform will be unavailable for use by the Customer. Scheduled Downtime will generally not exceed eight hours per calendar month and will be scheduled by Guardian during off-peak hours (based on Eastern Time). Guardian will notify Customer via email at least three business days before any periods of Scheduled Downtime expected to continue for two hours or more.

The duration of Scheduled Downtime is measured as the amount of elapsed time, in minutes, from when the Platform is not available to perform operations to the time when the Platform become available to perform operations. Daily system logs will be used to track Scheduled Downtime and any other Platform outages.

c. Unscheduled Downtime. Any period of time, measured in minutes, outside of the Scheduled Downtime when the Platform is not available to perform operations, excluding any unavailability caused by the failure of any third-party vendors, the Internet, any emergency or force majeure event, or any other reason beyond Guardian's control is considered "Unscheduled Downtime".

d. Failure To Meet Service Level Objectives. For Customers who are using the Platform subject to a separate, manually, or digitally executed agreement which includes prepayment by Customer for access to and use of the Platform, and in the event that Guardian fails to meet the Service Level Objectives, as defined herein, Customer and Guardian shall use all reasonable efforts to negotiate an amicable resolution in good faith within 20 business days of notification from the Customer of such a failure. Consideration for failure to meet service level objectives shall be limited to a.) potential discounts on Customer's renewal fees at the end of the current contract term or b.) a rebate to Customer in an amount equal to the pro-rated fees paid to Guardian for the period during which Guardian failed to meet service level objectives. Final consideration shall be determined by mutual agreement between the Parties.

14. USER REPRESENTATIONS AND WARRANTIES. You represent, warrant and agree that:

a. you are at least 18 years of age or older; and

b. you will not use (or plan, encourage or help others to use) the Platform for any purpose or in any manner that is prohibited by these Terms of Service or by applicable law. It is your responsibility to ensure that your use of the Platform complies with these Terms of Service and all applicable laws. If your information changes at any time, you are obligated to update your User Account to reflect those changes; and

c. you will abide by all local, state, national, and international laws and regulations applicable to User's use of the Platform; and

d. you will not send or store data on or to the Platform which violates the rights of any individual or entity established in any jurisdiction; and

e. you will not use the Platform for illegal, fraudulent, unethical or inappropriate purposes; and

f. you will not interfere or disrupt networks connected to the Platform or interfere with another's ability to access or use the Platform; and

g. you will not send unsolicited commercial email to other Users; and

h. you will not transmit or post any material that encourages conduct that could constitute a criminal offense or give rise to civil liability; User acknowledges and agrees that Guardian neither endorses the contents of any User communications or User Data or other User content nor assumes any responsibility for any infringement of third party intellectual property rights arising therefrom or any crime facilitated thereby; and

i. you will not post any information to a Platform that contains:

- **i.** copyrighted material (unless the User owns the copyright or has the owner's permission to post the copyrighted material); or
- **ii.** trade secrets (unless the User owns them or has the owner's permission to post them); or
- **iii.** material that infringes on or misappropriates any other intellectual property rights, or violates the privacy or publicity rights of others; or
- **iv.** anything that is discriminatory, sexually explicit, obscene, libelous, defamatory, threatening, harassing, abusive, or hateful; or
- **v.** anything that is embarrassing or offensive to another person or entity; and

j. you will not impersonate another person, living or dead;

k. you will not post false, inaccurate or misleading information, opinions or notices (commercial or otherwise) or chain letters; and

l. you will not post advertisements, or solicitations of business (including, but not limited to, email processors, any pyramid scheme or "club membership"); and

m. you will not delete or revise any material posted by any other person or entity; and

n. you will not provide system passwords or other log-in information for the Platform to any third party except those specifically authorized to access the Platform; and

o. you will not share non-public Guardian system features or content with any third party; and

p. you will not access the Platform in order to build, assist, or facilitate the assembly of a competitive product or service, to build a product using similar ideas, features, functions or graphics of the Platform, or to copy any ideas, features, functions or graphics of the Platform; and

q. you will not reverse engineer, decompile, disassemble or otherwise attempt to discover or directly access the source code or any underlying ideas or algorithms of any portions of the Platform or any underlying software or component thereof; and

r. you will not modify, create derivative works from, distribute, publicly display, publicly perform, or sublicense the Platform except as expressly permitted by this Agreement.

s. you will not rent, lease, distribute, sell, resell, assign, or otherwise transfer its rights to use the Platform; and

t. you will not use the Platform for the benefit of any third party; and

u. you will not remove any proprietary notices from the Platform or any other Guardian materials furnished or made available hereunder; and

v. you will not use the Platform to develop a database, online or similar database service, or other information resource of any kind (print, electronic or otherwise) for sale to, distribution to, display to or use by others or otherwise create or attempt to create a substitute or similar service or product through use of or access to any of the Platform or proprietary information related thereto; and

w. you will not store in a retrieval system accessible to the public, transfer, publish, distribute, display to others, broadcast, sell or sublicense the Platform, or any portion thereof; and

x. you will not pre-fetch, "crawl," "spider," or in any non-transitory manner store or cache any information obtain from the Platform (including results or any part or copy or derivative thereof), except that you may store data provided by the Platform for internal use so long as such storage is done in compliance with all applicable security requirements pertinent to User; and

y. you will not violate or attempt to violate the security of the Platform, including, without limitation:

- **i.** accessing data not intended for such User or logging into a server or account which the User is not authorized to access; or
- **ii.** attempting to probe, scan or test the vulnerability of a system or network or to breach security or authentication measures without proper authorization; or
- **iii.** attempting to interfere with service to any User, host or network, including, without limitation, via means of submitting a virus to the Platform, overloading, "flooding", "mail bombing" or "crashing"; or
- **iv.** sending unsolicited e-mail, including promotions and/or advertising of products or services; or

v. forging any TCP/IP packet header or any part of the header information in any e-mail or newsgroup posting. Violation of these Security Rules may result in civil or criminal liability. Guardian will investigate occurrences which may involve such violations and may involve, and cooperate with, law enforcement authorities in prosecuting Users who are involved in such violations.

15. INTELLECTUAL PROPERTY

a. **General.** Guardian respects the intellectual property of others. It is Guardian's policy to respond to claims of copyright and other intellectual property infringement. Guardian will promptly process and investigate notices of alleged infringement and will take appropriate actions under the Digital Millennium Copyright Act ("DMCA") and other applicable intellectual property laws. Upon receipt of notices complying with the DMCA, Guardian may act expeditiously to remove or disable access to any material claimed to be infringing or claimed to be the subject of infringing activity and may act expeditiously to remove or disable access to any reference or link to material or activity that is claimed to be infringing. Guardian will terminate access for Users who are repeat infringers.

b. **Notifying Guardian of Infringement.** To provide Guardian notice of an intellectual property infringement, you must provide a written communication to the attention of "Intellectual Property Infringement Notice" care of info@guardianalliancetechnologies.com that sets forth the information specified by the DMCA (http://www.copyright.gov/title17/92chap5.html#512). Please also note that you may be liable for damages (including costs and attorneys' fees) if you materially misrepresent that an activity is infringing your intellectual property.

c. **Providing Guardian with Counter-Notification.** If we remove or disable access to content in response to an infringement notice, we will make reasonable attempts to contact the owner or administrator of the affected Platform or content. If you feel that your material does not constitute infringement, you may provide Guardian with a counter notification by written communication to the attention of "Intellectual Property Infringement Notice" at info@guardianalliancetechnologies.com that sets forth all of the necessary information required by the DMCA (http://www.copyright.gov/title17/92chap5.html#512). Please note that you may be liable for damages (including costs and attorneys' fees) if you materially misrepresent that an activity is not infringing the copyrights of others. If you are uncertain whether an activity constitutes infringement, we recommended seeking advice of an attorney.

16. DISCLAIMERS AND LIMITATIONS ON GUARDIAN'S LIABILITY

a. **Allocation of Responsibility.** Guardian assumes no responsibility for Documents or other information posted by Users and no responsibility for the activities, omissions or other conduct of Users. Guardian acts as a portal for the online submission, collection, organization, review and evaluation of Applicant Documents and other information and has no obligation to screen communications or information in advance and is not

responsible for screening or monitoring Documents or other information posted by Users. If notified by a User of a Document or other information which allegedly does not conform to these Terms, Guardian may investigate the allegation and determine in good faith and in its sole discretion whether to remove or request the removal of such Document. Guardian has no liability or responsibility to Users for performance or nonperformance of such activities. Guardian may take any action with respect to User submitted information that it deems necessary or appropriate, in its sole discretion.

b. **No Endorsements By Guardian.** Nothing on the Platform shall be considered an endorsement, representation or warranty with respect to any User or third party, whether in regard to its web Platform, products, services, hiring, experience, employment or recruiting practices, or otherwise.

c. **California Residents**. If you are a California resident, you waive California Civil Code Section 1542, which says: "A general release does not extend to claims which the creditor does not know or suspect to exist in his or her favor at the time of executing the release, which if known by him or her must have materially affected his or her settlement with the debtor."

d. **Links to Other Platforms.** The Platform may contain links to third party web Platforms from time to time. These links are provided solely as a convenience to Users and not as an endorsement by Guardian of the contents on such third-party web Platforms. Guardian is not responsible for the content of linked third-party Platforms and does not make any representations regarding the content or accuracy of materials on such third-party web Platforms. Users hereby agree that, if Users decide to access linked third-party web Platforms, they do so at their own risk.

e. **Access To The Platform From Outside The United States.** Guardian contact information is listed on the Platform. Guardian makes no claims that the Content is appropriate or may be downloaded from territories outside of the United States. Access to the Content may not be legal by certain persons or in certain countries, and such persons have no right to access or use the Platform. If a User accesses Guardian from outside of the United States, they do so at their own risk and are responsible for compliance with the laws of their jurisdiction.

17. JURISDICTION

THIS AGREEMENT IS GOVERNED BY THE INTERNAL SUBSTANTIVE LAWS OF THE STATE OF CALIFORNIA, WITHOUT RESPECT TO ITS CONFLICT OF LAWS PRINCIPLES. JURISDICTION FOR ANY CLAIMS ARISING UNDER THIS AGREEMENT SHALL LIE EXCLUSIVELY WITH THE STATE OR FEDERAL COURTS IN THE STATE OF CALIFORNIA. THE SOLE RELATIONSHIP BETWEEN USERS AND GUARDIAN IS THAT OF INDEPENDENT CONTRACTORS. IF ANY PROVISION OF THIS AGREEMENT IS FOUND TO BE INVALID BY ANY COURT HAVING COMPETENT JURISDICTION, THE

INVALIDITY OF ALL OR PART OF A PROVISION SHALL NOT AFFECT THE VALIDITY OF THE REMAINING PARTS AND PROVISIONS OF THIS AGREEMENT, WHICH SHALL REMAIN IN FULL FORCE AND EFFECT. ALL PROVISIONS OF THIS AGREEMENT SHALL SURVIVE TERMINATION EXCEPT THOSE GRANTING ACCESS OR USE TO THE PLATFORM. UPON TERMINATION, USERS SHALL CEASE ALL USE AND ACCESS THEREOF IMMEDIATELY. USERS MAY NOT ASSIGN OR TRANSFER THEIR OBLIGATIONS UNDER THIS AGREEMENT. NO WAIVER OF ANY TERM OF THIS AGREEMENT SHALL BE DEEMED A FURTHER OR CONTINUING WAIVER OF SUCH TERM OR ANY OTHER TERM. EXCEPT AS EXPRESSLY PROVIDED BY GUARDIAN IN A PARTICULAR "LEGAL NOTICE," OR MATERIAL ON PARTICULAR WEB PAGES OF THE PLATFORM, THIS AGREEMENT WHERE APPLICABLE, CONSTITUTE THE ENTIRE AGREEMENT BETWEEN USERS AND/OR VISITORS AND GUARDIAN.

18. WARRANTY DISCLAIMERS

a. THE PLATFORM IS PROVIDED ON AN 'AS IS' BASIS WITHOUT ANY WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED. GUARDIAN, TO THE FULLEST EXTENT PERMITTED BY LAW, DISCLAIMS ALL WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT OF THIRD PARTIES' RIGHTS, AND FITNESS FOR A PARTICULAR PURPOSE. GUARDIAN MAKES NO WARRANTIES ABOUT THE ACCURACY, RELIABILITY, COMPLETENESS, OR TIMELINESS OF THE PLATFORM.

19. WITHOUT LIMITATION ON THE FOREGOING

a. GUARDIAN DOES NOT WARRANT THAT THE PLATFORM WILL OPERATE ERROR-FREE OR THAT THE PLATFORM AND/OR SERVERS ARE FREE OF COMPUTER VIRUSES OR OTHER HARMFUL MECHANISMS. IF YOUR USE OF THE PLATFORM RESULTS DIRECTLY OR INDIRECTLY IN THE NEED FOR SERVICING OR REPLACING EQUIPMENT OR DATA, GUARDIAN IS NOT RESPONSIBLE FOR THOSE COSTS.

b. GUARDIAN MAKES NO REPRESENTATIONS OR GUARANTEES REGARDING THE CONTENT OF THE PLATFORM, INCLUDING, BUT NOT LIMITED TO, BROKEN LINKS, INACCURACIES OR TYPOGRAPHICAL ERRORS.

c. GUARDIAN MAKES NO REPRESENTATIONS OR GUARANTEES REGARDING THE EFFECTIVENESS OF THE SERVICES OR TIMELINESS OF THE SERVICES IN MEETING YOUR EMPLOYMENT OBJECTIVES.

20. LIMITATION OF LIABILITY

a. USERS ASSUME ALL RESPONSIBILITY AND RISK FOR THEIR USE OF THE PLATFORM, THE INTERNET GENERALLY, AND THE DOCUMENTS THAT

USERS USE, POST, PROVIDE, COLLECT OR ACCESS AND FOR THEIR RESPECTIVE CONDUCT ON AND OFF THE PLATFORM.

b. IN NO EVENT SHALL GUARDIAN'S AGGREGATE LIABILITY, IF ANY, ARISING OUT OF OR IN ANY WAY RELATED TO CUSTOMER'S USE OF THE PLATFORM EXCEED THE AMOUNTS PAID TO GUARDIAN BY THE CUSTOMER, WITHOUT REGARD TO WHETHER SUCH CLAIM IS BASED IN CONTRACT, TORT (INCLUDING NEGLIGENCE), PRODUCT LIABILITY OR OTHERWISE AND NOTWITHSTANDING ANY FAILURE OF THE ESSENTIAL PURPOSE OF THE PLATFORM OR ANY LIMITED REMEDY HEREUNDER. IN NO EVENT WILL GUARDIAN'S OR ANY OF ITS OFFICERS, DIRECTORS, SHAREHOLDERS, EMPLOYEES, SUBSIDIARIES, AFFILIATES, AGENTS OR ADVERTISERS BE LIABLE FOR ANY DIRECT DAMAGES OF ANY KIND.

c. IN NO EVENT SHALL GUARDIAN OR ANY OF ITS OFFICERS, DIRECTORS, SHAREHOLDERS, EMPLOYEES, SUBSIDIARIES, AFFILIATES, AGENTS OR ADVERTISERS, BE LIABLE FOR ANY NON-DIRECT DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, INCIDENTAL AND CONSEQUENTIAL DAMAGES, LOST PROFITS, OR DAMAGES RESULTING FROM LOST DATA, LOST EMPLOYMENT OPPORTUNITY, OR BUSINESS INTERRUPTION) RESULTING FROM OR ARISING UNDER OR IN CONNECTION WITH THE PLATFORM OR THE USE OR ACCESS TO, OR THE INABILITY TO USE OR ACCESS, THE PLATFORM AND/OR ANY DOCUMENT, WHETHER BASED ON WARRANTY, CONTRACT, TORT, OR ANY OTHER LEGAL THEORY, AND WHETHER OR NOT GUARDIAN IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

d. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE LIMITATIONS SET FORTH IN THE PRECEDING PARAGRAPH MAY NOT APPLY TO YOU. IF ANY ARE HELD INAPPLICABLE OR UNENFORCEABLE FOR ANY REASON, THEN GUARDIAN'S MAXIMUM LIABILITY TO YOU FOR ANY NON-DIRECT TYPE OF DAMAGES SHALL BE LIMITED TO U.S. $200.00 IN THE AGGREGATE.

e. IN NO EVENT SHALL GUARDIAN (OR ANY OF ITS OFFICERS, DIRECTORS, SHAREHOLDERS, EMPLOYEES, SUBSIDIARIES, AFFILIATES, AGENTS OR ADVERTISERS), BE LIABLE FOR ANY DIRECT DAMAGES IN EXCESS IN THE AGGREGATE OF US $200.00.

f. DUE TO THE NATURE OF THIS AGREEMENT, IN ADDITION TO MONEY DAMAGES, YOU AGREE THAT GUARDIAN WILL BE ENTITLED TO EQUITABLE RELIEF UPON A BREACH OF THIS AGREEMENT BY YOU.

21. CONTACTING US

Questions and Notices. Questions concerning the use of the Platform should be directed to info@guardianalliancetechnologies.com. Notices to Guardian should be sent to the address listed

on the Platform. Guardian will send notices to the address submitted or to such other address as Guardian reasonably determines is an appropriate address.

Reporting User Conduct Violations. Inappropriate conduct can be reported by emailing: info@guardianalliancetechnologies.com

PRIVACY POLICY

Guardian Alliance Technologies, Inc. and its subsidiaries (collectively, "Guardian", "We" or "Our") provides this Privacy Policy to explain our data and security practices and policies on Guardian's cloud-based software Platform (the "Platform"). For the purpose of this Privacy Policy, Customers, Applicants, Employers who use the Platform are sometimes referred to generally and collectively as "Users".

This Privacy Policy describes the types of information we collect, how we use the information, with whom we share it, and the choices Users of the Platform can make about our collection, use and disclosure of Personal Information. The phrase "Personal Information" refers to information that personally identifies a User, such as User's personal name, address, telephone number, or email address. We also describe the measures we take to protect the security of a User's Personal Information and how Applicants can contact us about our privacy practices. When a User uses the Platform or provides us with information, they consent to our use and disclosure of the information we collect or receive as described in this Privacy Policy.

This Privacy Policy may be updated from time to time without prior notice to reflect changes in our data practices. We will post a prominent notice on our Platform to notify all Users of any significant changes to our Privacy Policy and indicate at the bottom of the notice when it was most recently updated. If we

make material changes to the policy that will affect previously collected Personal Information, Users will be notified and provided an opportunity to consent to the updated Privacy Policy.

Applicant Information

We may obtain information about Applicants from various sources, including directly from them via our Platform and/or when they call or email us. We also may obtain information about Applicants from our parent, affiliate or subsidiary companies, business partners and other third parties, as well as from publicly available information.

The type of Applicant information we collect includes:

- Personal Information provided by Applicants, such as Applicant usernames and passwords for access to the Platform, any/all documents uploaded by Applicant to our Platform, or collected from third party sources as described below.
- Publicly available data about Applicants obtained from third party Platform and sources, including profiles created by Applicants on other websites, or other information Applicants have publicly shared for the purpose of advertising or informing others about their background.
- Applicant Information entered or uploaded to the Platform by Employers such as Applicant related documents or Employer representative narratives entered for the purposes of evaluating Applicants employability.
- Applicant demographic information (such as zip or postal code, occupation, education and experience, and, if provided, age, gender and race or ethnicity). We collect this information either through the registration process, from the documents or information Applicants provide to our Platform, or in the manner described below.
- Platform behavior and preferences, and a record of the activities that any Users engage in on our Platform.
- Other details that Applicants may submit to us or that may be included in the information provided to us by third parties.

Technical Information

We collect technical information about Users' use of our Platform, as described below.

- Information about the devices our visitors use to access the Internet (such as the IP address and the device, browser and operating system type and other operating system support information).
- Dates and times of visits to our Platform.

- Information on actions taken on our Platform (such as page views, Platform navigation patterns and or profile activity).
- A general geographic location (such as country and city) from which a visitor accesses our Platform.

Use of User Information

We may use the information we obtain about Users to:

- Register, manage and maintain User accounts on the Platform.
- Provide products or services Users request.
- Maintain Applicant profiles, information, and documentation, and make it available to Employers through the Platform as described below in "Information We Share."
- Supplement an Applicant profile with publicly available information.
- Maintain a record of the documents or information Applicants provide to our Platform.
- Provide administrative notices or communications applicable to Users use of the Platform.
- Respond to User questions and comments and provide support.
- Contact Applicants and deliver information to them that, in some cases, is targeted to their interests (such as relevant services, educational or other career development opportunities); enable Applicants to communicate with us through our blogs, social networks and other interactive media; and solicit Applicant feedback and input. These communications will contain links for preference management and, where appropriate, unsubscribe links should Applicants decide they do not want to receive further communications.
- Manage User participation in our events and other promotions, where Users have signed up for such events and promotions.
- Operate, evaluate and improve our business and the products and services we offer.
- Analyze and enhance our marketing communications and strategies (including by identifying when emails we have sent to Users have been received and read).
- Analyze trends and statistics regarding use of our Platform, mobile applications and social media assets.
- Analyze trends and statistics about the job market and career mobility, locally and nationally, and provide these analytics to certain Users.

- Optimize our Platform search engine results and permit search engine access to public profile information.
- Protect against and prevent fraud, unauthorized transactions, claims and other liabilities, and manage risk exposure, including by identifying potential hackers and other unauthorized users.
- Enforce our Platform' Terms and Conditions.
- Comply with applicable legal requirements, court orders, legal proceedings, document requests, and industry standards and our policies.
- We also use non-personally identifiable information and certain technical information about computer hardware used by all Users accessing the Platform (including internet protocol addresses) in order to operate, maintain and manage the Platform. We collect this information by automated means, such as cookies and web beacons, as described in more detail below.
- If we seek to use information we obtain about Users in other ways, we will provide specific notice and request User consent at the time of collection.

Information We Share

- We share the information that we collect from Applicants or from third party sources with Employers and Integrated Service Providers.
- Employers may use Applicant information to contact Applicant's directly.
- When Applicant's provide documents or information through the Platform, the information and documents supplied by Applicants or shared through the Platform may become part of the Employer's database. Similarly, if an Applicant's profile on the Platform or documents that have been uploaded to the Platform by Applicant are downloaded by an Employer, Applicant information may become a part of the Employer's database. In these instances, the use of such information by the Employer will be subject to the privacy policy of that Employer, and Guardian is not responsible for the Employer's use of Applicant information.
- Guardian may share Applicant Information with our service providers who help us in the delivery of our own products and services to Employers. These service providers may only use or disclose the information as necessary to perform services on our behalf or as otherwise required by law.
- Guardian may disclose specific user information if/when Guardian determines, in good faith, that such disclosure is necessary to comply with the law, to cooperate with or seek assistance from law enforcement, to prevent a crime or protect national security, or to protect the interests or safety of Guardian or other Users of the Platform.
- Applicant Information that has been input or uploaded to the Platform may be passed on to a third party in the event of a transfer of ownership or assets or a bankruptcy or other corporate reorganization of Guardian.

Analytics

Guardian may combine certain non-personally identifiable Aggregate Data, as defined herein, or otherwise anonymized or de-identified data about our Users and use such data to prepare reports for Employers. Aggregate Data is used to analyze the characteristics of various populations and does not identify any specific individuals. Guardian may also use and share anonymized or de-identified data to track trends in the labor market as well as use of our products and services. Some Aggregate Data analytics reports can be used to better understand individual profiles.

Review, Update or Delete Users Account Information

Applicants may access, update and amend Personal Information included in their Guardian User Account at any time by logging into their account and making the necessary changes. Applicants may also delete their account from the Guardian Platform at any time by logging into their account and making an account deletion request. Deleting a Guardian account will not remove an Applicant's Personal Information or documents from the Guardian database. All Applicant Personal Information will remain in Guardian databases for an indefinite period of time.

Regardless of a successful account deletion, Employers and other parties who have gained access to Guardian databases, may have retained a copy of Applicant Personal Information and/or documents in their own files or databases. Guardian cannot control the retention, use or privacy of information or documentation that has been downloaded by third parties, and, Applicants will not be able to delete data held by third parties that already have accessed and downloaded Applicant Personal Information.

It may take up to thirty days to process an account deletion request.

Cookies

A "cookie" is a text file that Platform send to a visitor's computer or other Internet-connected device to uniquely identify the visitor's browser or to store information or settings in the browser. A "web beacon," is also called a Web bug or a pixel tag or a clear GIF. Used in combination with cookies, a Web beacon is an often-transparent graphic image, usually no larger than 1 pixel x 1 pixel, that is placed on a Web Platform or in an e-mail that is used to monitor the behavior of the person visiting the Platform or sending the e-mail.

Guardian uses cookies and other similar technologies for the convenience of our Users and some Guardian features or services may not function properly without cookies. Most Internet browsers provide for the erasure of cookies, blockage of cookies, or to prompt the computer user with a warning before a cookie is stored.

Guardian permits third party cookies on its Platform. For example, third party tools located on the Platform, including those that allow for social media sharing, may use cookies to remember user preference settings. Guardian also uses web analytics services provided by third parties, which use cookies to collect non-personal information about details of our users' visits to the Platform (including IP addresses) and the resources they access on the Platform. These third party web analytics services provide

Guardian with reports based on this information in order to help us understand how visitors engage with the Platform.

How We Protect Personal Information

Guardian observes and maintains a security program consistent with federal and state laws, regulations, and standards, including the CJIS Security Policy, as well as any other applicable policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB), combined with administrative, technical and physical safeguards designed to assist us in protecting the Personal Information we collect against accidental, unlawful or unauthorized destruction, loss, alteration, access, disclosure or use.

No electronic transmission, storage or processing of information can be entirely secure. Guardian cannot guarantee that the security measures in place will never be defeated or fail, or that those measures will always be sufficient or effective. Users of the Platform understand and agree that they bear the burden of all responsibility and risk for their use of the Platform, the internet generally, and the documents they post or access and for their conduct on and off the Platform.

To further protect themselves, Users and should safeguard their Guardian account usernames and passwords and not share that information with anyone. Users should also sign off of the Platform and close their browser window when they have finished their visit to the Platform. Guardian will never ask Users for their Guardian account username or password via email.

California, USA Residents

California law permits its residents to request and receive information about a business' disclosure of certain categories of Personal Information to other companies for their use in direct marketing. If Users are a California resident and a User of any of the Platform, Users can request a copy of this information from Guardian by sending an email to info@guardianalliancetechnologies.com. Please include User name and email address in email requests, and Usersr name and postal address in mail requests.

Children's Privacy

Guardian does not knowingly collect or solicit information from anyone under the age of 13. If Users are under 13, please do not use the Platform. In the event that we learn that we have collected personal information from a child under the age of 13, we will delete that information as quickly as possible.

How to Contact Us

Users can direct questions regarding this Privacy Policy to Guardian by emailing us at info@guardianalliancetechnologies.com. Please include Username and email address in email requests, and Usersname and postal address in mail requests.

Platform Activation Agreement

This Platform Activation Agreement ("**Agreement**") is made as of the "Effective Date" as set forth on page 4 hereof, by and between Guardian Alliance Technologies, Inc. ("**Guardian**"), located at 11 S. San Joaquin St., 8th Floor, Stockton, CA 95202, and:

_____

Customer Name (hereinafter referred to as "Customer") Officer or Authorized Representative Name and Title

with an address of

_____

Street Address, City, State, Zip

WHEREAS, Guardian has developed a cloud-based software platform (the "Guardian Platform") for use by law enforcement agencies in performing employment related background investigations; and

WHEREAS, Guardian has integrated Social Media Screening functionality into the Platform, the technology for which is provided by Fama Technologies, Inc. Fama is a third-party beneficiary of this Agreement; and

WHEREAS, the Customer desires to utilize the Platform, and Guardian desires to provide the Platform to the Customer pursuant to the terms and conditions of this Agreement.

A G R E E M E N T

NOW, THEREFORE, in consideration of the promises and covenants contained herein and the foregoing recitals, which are hereby incorporated into this Agreement, the Parties agree that the Terms of this Agreement shall govern Customer's of the Services as defined herein:

1. DEFINITIONS.

1.1 **"Account Administrator"** means an individual responsible for authorizing and managing all activity occurring under the Customer's Account.

1.2 "**Authorized User**" means an individual registered and identified by the Account Administrator by name who is authorized to use the Services on behalf of the Customer.

1.3 **"Terms of Service"** means, collectively, the Guardian Terms of Service and Guardian Privacy Policy. The Terms of Service may be updated from time to time at the discretion of Guardian and/or any Integrated Service providers as defined in the Guardian Terms of Service, respectively.

1.4 "**Social Media Screening**" means the collection of publicly available online Applicant information through the use of web-based software as a service software application owned by Fama Technologies, Inc. For the purpose of this Agreement, Social Media Screening is referred to as an "Integrated Service".

1.5 "**OnDemand Services**" means services available through the Platform which are available for a fee.

2. FCRA Compliance. Customer hereby acknowledges that Customer is solely responsible for its compliance with the Fair Credit Reporting Act ("FCRA") and any applicable state and local consumer reporting laws, in connection with its use of the Screening Service, if applicable.

3. Scope of Services.

3.1 Activation. By entering into this Agreement, Customer hereby requests that Guardian establish and activate a Customer Account on the Guardian Platform for use by Customer and its Authorized Users.

3.2 Free and OnDemand Features.

(a) Certain features of the Guardian Platform are complementary (free for all to Users). Other features are available on an OnDemand basis and if/when Customer uses these features, a fee will be charged to Customer. Current OnDemand Features include:

(i) Investigation Processing

(ii) Social Media Screening

(b) Customer is under no obligation to use the OnDemand Features. Notwithstanding the foregoing, upon entering into this Agreement, Guardian shall make the Investigation Processing Services and Screening Services available for Customer's use on an OnDemand basis subject to the Fees set forth in Section 3.3 herein.

3.3 Fees.

(a) Investigation Processing - $50 per investigation assigned to an investigator.

(b) Screening Service - $40 per screening.

3.4 Payment Terms. Customer will be invoiced at the beginning of each calendar month for all use of the Investigation Processing and Screening Service features during the previous calendar month. Invoices will be due upon receipt. Invoices shall be considered past due after 45 days from issuance.

3.5 Failure to Pay/Customer Conduct. Guardian reserves the right to deactivate Customer's access to the Platform if any payment is not received within 60 days of the invoice date.

3.6 Late Fee. Guardian reserves the right to charge a late fee of 1.5% per month on all invoices not paid within 60 days of issuance.

3.7 Additional Authorized Users. The Account Administrator shall have the authority and ability, through their User Account, to establish as many User Accounts for other individuals in their organization who are Authorized to use the Services on Customer's behalf. Additionally, the Account Administrator shall be responsible for deactivating Authorized User accounts when necessary.

3.8 Security. Each of the Parties agree to maintain a security program consistent with federal and state laws, regulations, and standards, including the CJIS Security Policy, as well as any other applicable policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

3.9 Terms of Service. By accessing and using the Services, Customer agrees to be bound by the Guardian Terms of Service. To the extent that any of the provisions of the Guardian Terms of Service differ from any of the provisions contained in this Agreement, the provisions contained herein shall supersede.

4. **Whitelist.** Customer hereby agrees to whitelist all domains as may be indicated by Guardian at any time during the Term of this Agreement, including but not limited to:

(a) guardian.network.org
(b) www.guardianalliancetech.com
(c) www.guardianalliancetechnologies.com

(Note: Content filtering systems in use by Customer, if any, may unexpectedly cut parts of html pages out of the user interface as well as some email traffic, lead to unexpected errors, broken links, unclickable buttons, partially loaded pages or other unintended/unpredictable behaviors with the Services. These issues are completely resolved by "whitelisting" all Guardian domains.)

5. **Intellectual Property Infringement.** Guardian shall indemnify, defend or, at its option, settle any third-party claim, suit or proceeding against customer to the extent based on a claim that the services (excluding any third-party software) infringes any united states patent, copyright, trademark or trade secret and Guardian shall pay any final judgment entered against customer in any claim, suit or proceeding or agreed to in settlement. Customer will notify Guardian in writing of the claim, suit or proceeding and give all information and assistance reasonably requested by Guardian or its designee. If use of the services is enjoined, Guardian may, at its option, do one or more of the following: (i) procure for customer the right to use the services, (ii) replace the services with other suitable services or products, or (iii) refund the unearned prepaid portion of the fees paid by customer for the services or the affected part thereof (if any). Guardian will have no liability under this section 5 to the extent a claim or suit is based upon (a) use of the Guardian Platform in combination with software not provided by Guardian if infringement would have been avoided in the absence of the combination, (b) modifications to the Guardian Platform not made by Guardian, if infringement would have been avoided by the absence of the modifications, or (c) use of any version other than a current release of the services, if infringement would have been avoided by use of a current release. This section 5 states Guardian's entire liability and customer's sole and exclusive remedy for intellectual property infringement or misappropriation claims.

6. **Counterparts.** This Agreement may be executed in any number of counterparts, and each executed counterpart shall have the same force and effect as an original instrument.

7. **Amendment.** The parties may amend this Agreement only by a written agreement of the parties that identifies itself as an amendment to this Agreement. If any part of this Agreement is found invalid or unenforceable that part will be enforced to the maximum extent permitted by law and the remainder of this Agreement will remain in full force.

8. **Marketing.** Guardian may use Customer's name as part of a general list of Customers and may refer to Customer as a user of the Services in its, general advertising and marketing materials.

9. **Invoicing Contact Information.**

Key contact for invoicing	
Email address for invoicing	
Phone number for invoicing	
Customer Address for Invoicing (if different from above)	

IN WITNESS WHEREOF, the parties are causing this Platform Activation Agreement to be executed by their duly authorized representatives.

Customer:	**Guardian Alliance Technologies, Inc.:**
_____	_____
Signature of officer or authorized representative	Signature of officer or authorized representative
_____	Adam Anthony COO
Print Name Title	Print Name Title
_____	
Effective Date	

From: Leslie Young
To: Chip Kirk
Subject: FW: Guardian and MMI
Date: Wednesday, April 21, 2021 3:06:29 PM

I think I sent this to you

From: Adam Anthony <adam@guardianalliancetechnologies.com>
Sent: Wednesday, April 21, 2021 2:07 PM
To: Leslie Young <leyoung@goodyearaz.gov>
Cc: Kim Johnson <kim@guardianalliancetechnologies.com>
Subject: Re: Guardian and MMI

Hi Leslie,

What appears below is a narrative prelude to the attached PDF which contains just the essential facts. I'd be happy to speak with anyone who has questions about this matter, just give me a shout if that is desired.

As you know by now, Miller Mendel has filed a lawsuit against Oklahoma City PD, claiming that OKC is infringing in a patent owned by MMI by virtue of OKC using the Guardian software. This suit was initiated against OKC as a result of OKC PD choosing Guardian over MMI in an open bidding process. Guardian is providing the legal defense for Oklahoma City as a Guardian customer and although Guardian is not a formal party to the case, Guardian's software is the central focus.

This case has been ongoing for over two years and whenever MMI learns the identity of an agency using or contemplating the use of Guardian, they have systematically embarked upon a campaign of threats and intimidation in an effort to frighten agencies away from using the Guardian Platform.

Not addressed in the attached, but of interest, is related activity by MMI which involves the distribution of misleading information about Guardian's one-of-a-kind "NAIC"(central applicant database). Specifically, MMI is suggesting that Guardian is sharing applicant data with multiple agencies in violation of data privacy laws and guidelines. This is absolutely false. At no time does Guardian share applicant data with anyone, and in no way does the Guardian NAIC breach any data privacy laws or guidelines.

Guardian is a Select Tier Partner of AWS and a member company of their Justice Reform Program. The Guardian Platform and its workings have been vetted not only by AWS, but by numerous law enforcement agencies across the country and the NAIC has never received anything other than wide positive acclaim.

The OKC case is expected to continue well into 2021. At the conclusion we expect the MMI patent to be invalidated. As the attached reflects, the patent is definitively invalid and unenforceable for a number of reasons. If necessary, we would be happy to put you in touch with the lawyers who represent OKC in this matter who can corroborate all information contained herein.

Please let me know if you have any questions. As mentioned above, I'd be happy to hop on a call to discuss, as necessary.

Regards,
Adam

Adam Anthony, COO
Guardian Alliance Technologies, Inc.
11 S. San Joaquin St., 8th Floor, Stockton, CA 95202
www.guardianalliancetechnologies.com
e: adam@guardianalliancetechnologies.com
[redacted]

[redacted]

Trials@uspto.gov
571-272-7822

Paper 23
Date: March 26, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GUARDIAN ALLIANCE TECHNOLOGIES, INC.,
Petitioner,

v.

TYLER MILLER,
Patent Owner.

IPR2020-00031
Patent 10,043,188 B2

Before SALLY C. MEDLEY, DAVID C. MCKONE,
and JOHN R. KENNY, *Administrative Patent Judges*.

MCKONE, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. Background and Summary

Guardian Alliance Technologies, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1, 5, 9, and 15 of U.S. Patent No. 10,043,188 B2 (Ex. 1001, "the '188 patent"). Pet. 1. Petitioner indicates that Guardian Alliance Holdings, Inc., and the City of Oklahoma City are real parties-in-interest. *Id.* Tyler Miller ("Patent Owner") filed a Preliminary Response (Paper 7, "Prelim. Resp.").

We have authority to determine whether to institute an *inter partes* review. *See* 35 U.S.C. § 314; 37 C.F.R. § 42.4(a) (2019). The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides that an *inter partes* review may not be instituted "unless . . . there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Under the circumstances of this case, for the reasons explained below, we deny institution of an *inter partes* review of the '188 patent.

Petitioner also filed a Motion to Correct a Clerical Mistake in the Petition Under 37 C.F.R. § 42.104(c) (Paper 11, "Mot. to Correct") and Patent Owner filed a Motion to Terminate IPR Proceeding (Paper 10, "Mot. to Terminate").

B. Related Matters

The parties indicate that Patent Owner's exclusive licensee, Miller Mendel, Inc., has asserted the '188 patent against Petitioner's real party-in-interest, the City of Oklahoma City, in *Miller Mendel, Inc. v. City of Oklahoma City*, Case No. 5:18-cv-00990-M (W.D. Ok.). Pet. 1; Paper 3, 1.

C. The '188 Patent

The '188 patent describes software related to facilitating the process of performing background investigations on, for example, job applicants. Ex. 1001, 1:14–16. Figure 1, reproduced below, illustrates an example:

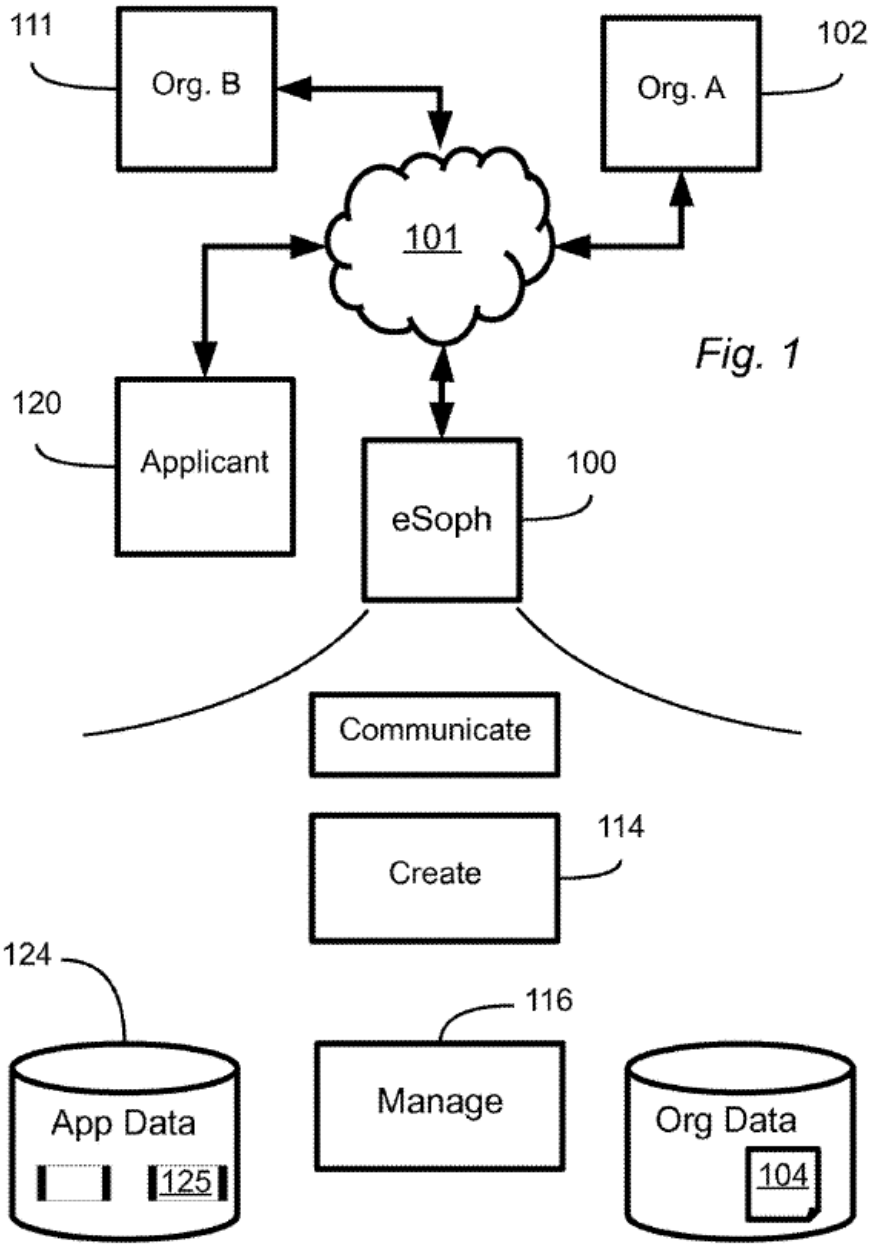


Figure 1 is a block diagram of core components of a background investigation management system. *Id.* at 1:48–51.

Using software system 100, Organization A can create and customize electronic documents 104 to send to applicants, who complete documents via software system 100 and return them to software system 100. *Id.* at 4:5–9. Software system 100 includes document creation component 114 and document management component 116. *Id.* at 4:9–11. In one feature, applicant information 124 can be shared between Organization A and Organization B. *Id.* at 4:15–21. Organization A can send electronic documents 104 to applicant 120 by emailing applicant 120 a link to log into software system 100. *Id.* at 5:29–35. Organization A can send and receive documents (e.g., questionnaires) to and from references (e.g., relatives, employers, co-workers, and neighbors) in a similar manner. *Id.* at 8:31–39. The software system also can include a feature that will retrieve law enforcement and court names, addresses, and phone numbers for a pre-defined radius around an address for the applicant, the applicant's employer, or the applicant's relatives. *Id.* at 9:48–52.

Claim 1, reproduced below, is illustrative of the invention:

> 1. A method for a computing device with a processor and a system memory to assist an investigator in conducting a background investigation of an applicant for a position within a first organization, comprising the steps of:
>
> receiving a first set of program data comprising information identifying the applicant, the position, the first organization, and the investigator;
>
> storing a new applicant entry in the system memory, the new applicant entry associated with the first set of program data;
>
> transmitting an applicant hyperlink to an applicant email address associated with the applicant, the applicant hyperlink for viewing an applicant set of electronic documents;

receiving an applicant electronic response with a reference set of program data, wherein the reference set of program data comprises information regarding a reference source, wherein the reference source is a person, the program data including a reference email address associated with the reference source;

determining a reference class of the reference source based on the reference set of program data;

selecting a reference set of electronic documents based on the reference class of the reference source;

transmitting a reference hyperlink to the reference email address, the reference hyperlink for viewing the reference set of electronic documents;

receiving a reference electronic response to the reference set of electronic documents from the reference source;

storing the reference electronic response in the system memory, associating the reference electronic response with the new applicant entry; and

generating a suggested reference list of one or more law enforcement agencies based on an applicant residential address.

D. Evidence

Petitioner relies on the references listed below.

Reference		Date	Exhibit No.
Background Solutions	Background Solutions, LLC, Background Assistant video	2009	1002, 1027[1]
LaPasta	US 2005/0033633 A1	pub. Feb. 10, 2005	1003
POBITS	Peace Officer Background Investigation Tracking System and Manual	Feb. 1, 2011	1004
ADP	US 2008/0306750 A1	pub. Dec. 11, 2008	1015

Petitioner also relies on the Declaration of Thomas Ward (Ex. 1009) and the Declaration of Kingsley Klosson (Ex. 1014).

E. The Asserted Grounds of Unpatentability

Claims Challenged	35 U.S.C. §	Reference(s)/Basis
1, 5, 9, 15	103	Background Solutions, LaPasta
1, 5, 9, 15	103	POBITS, ADP

[1] Exhibit 1002 is subject to Petitioner's Motion to Correct, in which Petitioner seeks to substitute the video of Exhibit 1027 ("the 2009 Video") as a correction to the video of Exhibit 1002 ("the 2012 Video"). Mot. to Correct 1. Patent Owner opposes (Paper 16, "Opp. to Mot. to Correct"). Concurrently, Patent Owner files its Motion to Terminate based on Petitioner's failure to serve the correct video with the Petition by the bar date under 35 U.S.C. § 315(b). Petitioner opposes (Paper 12, "Opp. to Mot. to Terminate").

II. ANALYSIS

A. Claim Construction

For petitions filed after November 13, 2018, we construe claims "using the same claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent." 37 C.F.R. § 42.100(b) (2019). *See also Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc).

Petitioner proposes several claim terms for construction, essentially asking us to adopt constructions proposed by Patent Owner in the related district court litigation. Pet. 13–17. Petitioner also proposes constructions for two other terms not addressed in the district court litigation. *Id.* at 17–18. Patent Owner does not address claim construction in the Preliminary Response. Based on the record before us, we do not find it necessary to provide any express claim constructions. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (noting that "we need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy'") (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)).

B. Printed Publication Status of References

Patent Owner contends that neither Background Solutions nor POBITS qualifies as a printed publication and, thus, neither is prior art to the '188 patent. Prelim. Resp. 13–14, 19–34.

Whether a reference qualifies as a "printed publication" is a legal conclusion based on underlying factual findings. *See Nobel Biocare Servs.*

AG v. Instradent USA, Inc., 903 F.3d 1365, 1375 (Fed. Cir. 2018) (citing *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018)). The underlying factual findings include whether the reference was publicly accessible. *See id.* (citing *In re NTP, Inc.*, 654 F.3d 1279, 1296 (Fed. Cir. 2011)).

"The determination of whether a reference is a 'printed publication' under 35 U.S.C. § 102(b) involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public." *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). "Because there are many ways in which a reference may be disseminated to the interested public, 'public accessibility' has been called the touchstone in determining whether a reference constitutes a 'printed publication' bar under 35 U.S.C. § 102(b)." *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016) (quoting *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986)). "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc*., 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

What constitutes a "printed publication" must be determined in light of the technology employed. *See* S*amsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019) (citing *In re Wyer*, 655 F.2d 221, 226 (CCPA 1981)). Public accessibility requires more than technical accessibility. *See id.* (citing *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 773 (Fed. Cir. 2018)). "[A] work is not publicly

accessible if the only people who know how to find it are the ones who created it." *Id.* at 1372. On the other hand, "a petitioner need not establish that specific persons actually accessed or received a work to show that the work was publicly accessible." *Id.* at 1374. "In fact, a limited distribution can make a work publicly accessible under certain circumstances." *Id.* (quoting *GoPro, Inc. v. Contour IP Holding LLC*, 908 F.3d 690, 694 (Fed. Cir. 2018)).

"To prevail in a final written decision in an inter partes review, the petitioner bears the burden of establishing by a preponderance of the evidence that a particular document is a printed publication." *Hulu, LLC v. Sound View Innovations, LLC*, Case IPR2018-01039 (PTAB Dec. 20, 2019) (Paper 29) (precedential), slip op. at 11. "[A]t the institution stage, the petition must identify, with particularity, evidence sufficient to establish a reasonable likelihood that the reference was publicly accessible before the critical date of the challenged patent and therefore that there is a reasonable likelihood that it qualifies as a printed publication." *Id.* at 13.

1. Background Solutions

According to Petitioner, Background Solutions is a video demonstration of a Background Assistant background investigation system that was displayed at trade seminars as early as mid-2009 and publicly accessible on the Internet at Background Solutions, LLC's website no later than November 23, 2009. Pet. 4–5. Patent Owner argues that the video in Exhibit 1002 has several indications that it was created no earlier than 2012 and, thus, is not prior art to the '188 patent. Prelim. Resp. 14–19. As noted above, Petitioner filed a Motion to Correct Exhibit 1002, seeking to substitute Exhibit 1027 in its place. Petitioner contends that it erroneously

marked and uploaded the 2012 Video as Exhibit 1002 instead of the 2009 Video it sought to upload and now offers in substitution. Mot. to Correct 1. We grant Petitioner's Motion to Correct for the limited purpose of considering the 2009 Video (Exhibit 1027). For the reasons that follow, however, Petitioner has not shown a reasonable likelihood that the 2009 Video qualifies as a printed publication.

Petitioner offers two theories as to why the 2009 Video was publicly accessible in mid-2009. First, Petitioner argues that Tom Ward, the founder and co-owner of Background Solutions, LLC, presented the 2009 Video at national background investigation seminars. Pet. 19. Second, Petitioner contends that the 2009 Video was publicly accessible on Background Solutions, LLC's website, and that at the national background investigation seminars, Mr. Ward distributed pamphlets with the URL to that website. *Id.* According to Petitioner, "an oral presentation accompanied by distribution or display at a conference can establish a reference as a 'printed publication.'" *Id.* at 20 (citing *Klopfenstein*, 380 F.3d at 1347–52).

> In *Klopfenstein*, a fourteen-slide poster presentation
>
> was shown to a wide variety of viewers, a large subsection of whom possessed ordinary skill in the art of cereal chemistry and agriculture. Furthermore, the reference was prominently displayed for approximately three cumulative days at [American Association of Cereal Chemists] and the [Agriculture Experiment Station] at Kansas State University. The reference was shown with no stated expectation that the information would not be copied or reproduced by those viewing it.

380 F.3d at 1350. According to the Federal Circuit, in determining whether the presentation was publicly accessible,

> [t]he factors relevant to the facts of [the *Klopfenstein*] case [were]: the length of time the display was exhibited, the

> expertise of the target audience, the existence (or lack thereof) of reasonable expectations that the material displayed would not be copied, and the simplicity or ease with which the material displayed could have been copied.

Id.

In support of its arguments, Petitioner offers the testimony of Mr. Ward. Mr. Ward testifies that Background Solutions began developing the Background Assistant™ software in 2006, "with product sales being generated in mid-2009 based on company records." Ex. 1009 ¶ 5. Such "company records" are not part of the record in this proceeding. According to Mr. Ward, the product development team for the Background Assistant software "outsourced the production of a power point video demonstration (Ex. 1002) of Background Assistant™ background investigation software for marketing purposes." *Id.* ¶ 6. Mr. Ward testifies that he "played the Background Assistant™ product video (Ex. 1002) for the seminar attendees" and "had embedded the video in my background investigation seminar power point presentation." *Id.* ¶ 7. According to Mr. Ward, he "used the video to explain to seminar attendees that an electronic solution for police background investigations was available through the Background Assistant software." *Id.* Petitioner argues that "Mr. Ward's presentation and demonstration of the Background Solutions video to a national conference of background investigators, i.e. those interested and skilled in the subject matter, qualifies it as a printed publication." Pet. 20–21.

In response, Patent Owner argues that Mr. Ward does not identify any specific seminars at which he presented the 2009 Video, does not present any evidence of the backgrounds of the attendees of the seminars (or whether any attendees had backgrounds in software development), and does not address the length of the seminar presentation. Prelim. Resp. 21.

According to Patent Owner, "Ward does not identify a single conference by name or date," and "Petitioner provides no corroborating evidence regarding the audience size or the number of [persons of ordinary skill in the art] that attended any alleged presentation." *Id*. at 25.

We agree with Patent Owner. At the petition stage, Petitioner must identify "with particularity" the evidence it contends shows a reasonable likelihood that the 2009 Video is a printed publication. *Hulu*, at 13. Petitioner's evidence lacks particularity. Although Mr. Ward testifies that he presented the 2009 Video at "law enforcement and background investigation seminars," he does not testify as to how many such seminars he presented at, when or where those seminars were, who attended the seminars, or who watched the 2009 Video at the seminars.[2] Ex. 1009 ¶¶ 7–9. Rather, his testimony is vague and conclusory.

Petitioner cites *Klopfenstein* for the proposition that an oral presentation accompanied by a display at a conference can be enough to establish that a reference is a printed publication. Pet. 20 (citing *Klopfenstein*, 380 F.3d at 1347–52). However, Petitioner's showing does not address any of the factors the *Klopfenstein* court considered in deciding that the reference in that case was a printed publication. Here, for example, Mr. Ward does not testify as to when or where he presented the 2009 Video,

[2] Mr. Ward testifies that "[a]mongst other customers, Background Solutions provided the Background Assistant™ product and background investigation services to King County (WA) Sheriff's Department." Ex. 1009 ¶ 12. However, Mr. Ward does not testify that he showed the video to the customer, or that the customer attended a seminar. He also does not testify as to when King County was a customer or whether it was prior to the effective filing date of the '188 patent. Thus, this testimony does not support any of Petitioner's arguments.

the length of time it was exhibited, or the expertise of the seminar audiences. *See Klopfenstein*, 380 F.3d at 1350. Moreover, because he does not provide any details about seminar dates or attendees, Mr. Ward does not indicate whether he presented the 2009 Video at any seminar prior to April 6, 2012, the earliest filing date on the face of the '188 patent,[3] or whether any skilled artisans[4] attended those seminars. Ex. 1009 ¶¶ 7–9.

Petitioner further argues that Background Solutions, LLC, made the 2009 Video accessible on its website no later than November 23, 2009. Pet. 21–24. Mr. Ward testifies that, at the seminars discussed above, he "distributed a product brochure advertising the Background Assistant™ background investigation software, which provides the URL for the Background Solutions website, www.backgroundsolutions.com," and that the 2009 Video "was made available to the public at the URL www.backgroundsolutions.com," which "contained a link to the same Background Assistant™ product video presented at the above-described law enforcement and background investigation seminars." Ex. 1009 ¶¶ 8–9.

Patent Owner argues that "Petitioner provides no evidence that Ex. 1002 was distributed to any person at said unnamed conferences" and

[3] Patent Owner seeks to file a Petition for Correction of Priority Claim to claim the benefit of an earlier-filed provisional application. Paper 9. An earlier priority date would not affect our analysis, as Petitioner has not shown that the 2009 Video was publicly accessible before the later filing date on the face of the patent.

[4] The parties dispute the level of skill of a skilled artisan. Pet. 5–6; Prelim. Resp. 6–7. We need not resolve this dispute, as Mr. Ward does not testify as to the backgrounds of any seminar attendees. Thus, we are unable to ascertain whether any seminar attendee had either of the two proffered levels of skill.

that "there is no corroborating proof of what, if anything was on Ward's website." Prelim. Resp. 27.

For a reference posted to a website, there are multiple ways that Petitioner could show that the reference was publicly accessible. For example, Petitioner could show that the website was indexed, through search engines or otherwise. *See Blue Calypso*, 815 F.3d at 1349. Petitioner and Mr. Ward, however, offer no evidence of how Background Solutions, LLC's website was indexed, if at all.

Petitioner also could show that the record indicates that, despite a lack of indexing, the website was well known to the community interested in the subject matter of the reference. *See Voter Verified, Inc. v. Premier Election Solutions, Inc.*, 698 F.3d 1374, 1380–81 (Fed. Cir. 2012) ("[T]he uncontested evidence indicates that a person of ordinary skill interested in electronic voting would have been independently aware of the Risks Digest as a prominent forum for discussing such technologies. And upon accessing the Risks Digest website, such an interested researcher would have found the Benson article using that website's own search functions and applying reasonable diligence."). Petitioner does not allege, and Mr. Ward's testimony does not suggest, that Background Solutions, LLC's website was a well-known forum for the community interested in the subject matter of the 2009 Video. Pet. 19–24; Ex. 1009. *See also Blue Calypso*, 815 F.3d at 1349–50 ("[I]n contrast to *Voter Verified*, the present case lacks any testimonial evidence that a person interested in e-commerce and peer-to-peer marketing would be independently aware of the web address for Dr. Ratsimor's personal page. In other words, there was no evidence that the ordinarily skilled artisan would know of Dr. Ratsimor's personal webpage or its web address.").

Petitioner also could show that the 2009 Video was publicly accessible through the use of a "research aid," such as a published article or patent that made reference to the 2009 Video. *See Blue Calypso*, 815 F.3d at 1350. The research aid would need to provide "a sufficiently definite roadmap" to the 2009 Video, although "[a]n adequate roadmap need not give turn-by-turn directions, but should at least provide enough details from which we can determine that an interested party is reasonably certain to arrive at the destination: the potentially invalidating reference." *Id.* To that end, as noted above, Mr. Ward testifies that he distributed at seminars product brochures with the URL to Background Solutions, LLC's website, where the 2009 Video could be found. Ex. 1009 ¶¶ 8–9. Petitioner argues that "[t]he URL for the homepage of the website, www.backgroundsolutions.com, was distributed to all of the attendees at these background investigation seminars," and, thus, a skilled artisan "could have gained access to the Backgrounds Solutions . . . demonstration video describing Background Assistant™, through either (1) attendance at the national background investigation seminar, or (2) the Background Solutions publicly accessible website." Pet. 24. However, as also noted above, Mr. Ward does not testify as to when or where the seminars occurred or who attended them. Thus, the evidence does not show who, if anyone, would have been given such a brochure or when they would have received it.

We further note that Mr. Ward does not testify as to when the 2009 Video was posted on Background Solutions, LLC's website, or whether it would have been posted before April 6, 2012. Ex. 1009. Nevertheless, Petitioner argues that the Internet Archive, in particular Exhibit 1023, supports Mr. Ward's testimony and establishes that the 2009 Video was

posted before November 23, 2009. Pet. 23. A portion of Exhibit 1023 is reproduced below:

The above figure is a portion of an Internet Archive capture of the webpage www.backgroundsolutions.com/index.html, purporting to have been captured on November 23, 2009. Ex. 1023, 1.

Petitioner does not state with specificity where the 2009 Video can be found in this capture. However clicking on the "Background Assistant" icon leads to a product brochure; thus, we presume that Petitioner intended to point us to the "Demo" icon. As Patent Owner argues, however, clicking on the "Demo" icon leads to a blank webpage, without any indication that the 2009 Video was reachable via that webpage. Prelim. Resp. 21–23. Thus,

Petitioner's Internet Archive capture (Ex. 1023) does not provide evidence that the 2009 Video would have been available on Background Solutions, LLC's website prior to April 6, 2012.

In sum, we have considered Petitioner's evidence, including Mr. Ward's testimony (Ex. 1009) and Petitioner's Internet Archive capture (Ex. 1023), and conclude that Petitioner has not shown a reasonable likelihood that the 2009 Video was publicly accessible before April 6, 2012. Neither Petitioner nor Mr. Ward provide enough specificity to determine when the 2009 Video was presented at seminars, when those seminars occurred, or who attended the seminars. Thus, even if we credit Mr. Ward's testimony, it is not sufficient to show that Mr. Ward presented the 2009 Video to skilled artisans at a seminar prior to April 6, 2012. The evidence also does not support a finding that the 2009 Video was posted to Background Solutions, LLC's website prior to April 6, 2012, or, even if it was, that a skilled artisan exercising reasonable diligence would have been able to locate it. Thus, on this record, Petitioner has not shown a reasonable likelihood that the 2009 Video qualifies as a printed publication and, accordingly, that it qualifies as prior art to the '188 patent. Therefore, on this record, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 1, 5, 9, and 15 would have been obvious over Background Solutions (i.e., the 2009 Video) and LaPasta.

2. POBITS

POBITS is an Internet Archive capture of an online user's manual. As Petitioner notes (Pet. 24), POBITS bears a copyright date of 2010. *See, e.g.,* Ex. 1004, 1. Petitioner contends that the testimony of Mr. Klosson, along with the Internet Archive capture, shows that POBTIS was available at

the website www.esdevllc.com/pobits/help/index.html no later than December 31, 2010. Pet. 24.

Mr. Klosson testifies that he "began developing one of [his] products, the Peace Officer Background Investigation Tracking System ('POBITS'), in 2005 and developed a web-based version of the product in 2008, which went live in 2010." Ex. 1014 ¶ 6. According to Mr. Klosson, "[t]he POBITS product and system has been offered for sale since 2005 and the modernized system since 2010." *Id.* ¶ 9. Mr. Klosson testifies that "[i]n conjunction with marketing and offering the POBITS product for sale, between 2005 and 2010, [he] posted a POBITS online user manual and technical reference (Ex. 1004) to [his] company's website," and that the Internet Archive corroborates that POBITS was available to the public no later than February 1, 2011. *Id.* ¶ 10. Mr. Klosson further testifies that Exhibit 1004 (POBITS) "is a collection of screenshots of the Internet Archive (http://web.archive.org) crawls or snapshots of the online POBITS user manual and technical reference, taken on February 1, 2011" and "correctly depicts the online POBITS user manual and technical reference as of February 1, 2011." *Id.* ¶ 11. Mr. Klosson concludes that "Ex. 1004 is a true and correct copy of the POBITS online user's manual that was available to the public through the Essential Software Development website no later than February 1, 2011." *Id.* ¶ 12.

Even if we credit Mr. Klosson's testimony, it is insufficient to show a reasonable likelihood that POBITS was publicly accessible. As explained above, to establish public accessibility of a reference alleged to be available on a website, a petitioner could show that the website was indexed, through search engines or otherwise. *See Blue Calypso*, 815 F.3d at 1349. Petitioner and Mr. Klosson, however, offer no evidence of how Essential Software

Development's website was indexed, if at all. A petitioner also could show that the website was well known to the community interested in the subject matter of the reference. *See Voter Verified*, 698 F.3d at 1380–81. Neither Petitioner nor Mr. Klosson has alleged facts that would support a finding that Essential Software Development's website was well known to the community interested in the subject matter of POBITS. *See* Pet. 24; Ex. 1014. Nor do Petitioner or Mr. Klosson allege that some other public document could serve as a "research aid" that would lead skilled artisans to POBITS. *See Blue Calypso*, 815 F.3d at 1350.

Other than arguing the existence of POBITS on a public website on February 1, 2011, Petitioner makes no allegations that would support a finding of public accessibility. Petitioner's theory is, simply, that "[a]n interested [person of ordinary skill in the art] could have gained access to the POBITS printed publication through the publicly accessible website." Pet. 24. Even if we accept this as true, it is not sufficient to show public accessibility. *See Blue Calypso*, 815 F.3d at 1349–50.

Patent Owner also argues that the February 1, 2011, archive date only applies to the outer "frame" of POBITS, which essentially depicts a selectable table of contents, and not to the individual pages contained within the frame. Prelim. Resp. 29–33. We need not reach this argument. As explained above, even if we assume that the entirety of POBITS was available on a public website on February 1, 2011, that, without more, is insufficient to show public accessibility. *See Blue Calypso*, 815 F.3d at 1349–50.

As noted above, Petitioner also points out that POBITS carries a copyright date of 2010. *Id.* As Patent Owner notes (Prelim. Resp. 33–34), however, a copyright date does not, by itself, establish that a document was

published by the copyright date. We may consider indicia such as copyright dates as "part of the totality of the evidence." *Hulu*, at 17–18. In this case, a copyright date of 2010 would tend, at most, to corroborate that POBITS was posted on a public website around that time. As explained above, that, by itself, is not sufficient to show a reasonable likelihood that POBITS was publicly accessible. *See Blue Calypso*, 815 F.3d at 1349–50.

In sum, Petitioner's evidence, at most, supports a finding that POBITS was posted on a public website by February 1, 2011. That is insufficient to show that POBITS was publicly accessible by that date. On this record, we conclude that Petitioner has not shown a reasonable likelihood that POBITS is a printed publication and, accordingly, prior art to the '188 patent. Therefore, on this record, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 1, 5, 9, and 15 would have been obvious over POBITS and ADP.

C. Petitioner's Motion to Correct and Patent Owner's Motion to Terminate

We grant Petitioner's Motion to Correct for the limited purpose of considering Exhibit 1027, the 2009 Video, in the context of denying institution. As explained above, however, Petitioner still cannot show, on a record that includes Exhibit 1027, that Background Solutions is prior art to the '188 patent.

Because we deny the Petition for the reasons given above, it is not necessary to decide Patent Owner's Motion to Terminate. We dismiss that motion as moot.

III. CONCLUSION

Petitioner has not shown a reasonable likelihood that either Background Solutions or POBITS is prior art to the '188 patent. Thus, Petitioner has not demonstrated a reasonable likelihood that it would prevail in showing that claims 1, 5, 9, and 15 would have been obvious over Background Solutions and LaPasta or that claims 1, 5, 9, and 15 would have been obvious over POBITS and ADP.

Petitioner's Motion to Correct (Paper 11) is granted for the purpose of considering Exhibit 1027.

Patent Owner's Motion to Terminate (Paper 10) is dismissed as moot.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED that the Petition is *denied* as to the challenged claims of the '188 patent, and no *inter partes* review is instituted; and

FURTHER ORDERED that Petitioner's Motion to Correct a Clerical Mistake in the Petition Under 37 C.F.R. § 42.104(c) (Paper 11) is *granted* for the purpose of considering Exhibit 1027; and

FURTHER ORDERED that Patent Owner's Motion to Terminate IPR Proceeding (Paper 10) is *dismissed* as moot.

FOR PETITIONER:

Jordan Sigale
Douglas Sorocco
DUNLAP CODDING, P.C.
jsigale@dunlapcodding.com
dsorocco@dunlapcodding.com

FOR PATENT OWNER:

Richard McLeod
MCLEOD LAW LLC
law@rickmcleod.com

Kurt Rylander
RYLANDER & ASSOCIATES PC
Rylander@rylanderlaw.com

Trials@uspto.gov
571-272-7822

Paper 27
Date: July 27, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GUARDIAN ALLIANCE TECHNOLOGIES, INC.,
Petitioner,

v.

TYLER MILLER,
Patent Owner.

IPR2020-00031
Patent 10,043,188 B2

Before SALLY C. MEDLEY, DAVID C. MCKONE,
and JOHN R. KENNY, *Administrative Patent Judges*.

MCKONE, *Administrative Patent Judge*.

DECISION
Denying Petitioner's Request on Rehearing of Decision on Institution
37 C.F.R. § 42.71(d)

I. INTRODUCTION

Guardian Alliance Technologies, Inc. ("Petitioner") filed a Petition (Paper 1, "Pet.") requesting *inter partes* review of claims 1, 5, 9, and 15 of U.S. Patent No. 10,043,188 B2 (Ex. 1001, "the '188 patent"). Pet. 1. Tyler Miller ("Patent Owner") filed a Preliminary Response (Paper 7, "Prelim. Resp."). The Petition raised two grounds, the first based in part on the Background Solutions[1] video and the second based in part on the POBITS[2] reference (Ex. 1004). Pet. 4. Upon consideration of the Petition and the Preliminary Response, as to the first ground, we determined that Petitioner had not shown sufficiently that Background Solutions was publicly accessible, and, thus, prior art to the '188 patent. Paper 23 ("Dec."), 9–17. As to the second ground, we determined that Petitioner had not shown sufficiently that POBITS was publicly accessible, and, thus, prior art to the '188 patent. Dec. 17–20.

Petitioner asks us to reconsider our determinations that Background Solutions and POBITS were not publicly accessible and, thus, were not prior art to the '188 patent. Paper 24 ("Req."). For the reasons given below, we decline to modify our Decision.

---

[1] Petitioner submitted Exhibit 1002 as the Background Solutions video and subsequently moved to correct it through submission of a substitute video (Exhibit 1027), a motion that Patent Owner opposed. Papers 11 (Motion to Correct), 16 (Opposition). Concurrently, Patent Owner moved to terminate based on the incorrectly submitted Exhibit 1002. Papers 10 (Motion to Terminate), 12 (Opposition). We granted Petitioner's Motion to Correct for the limited purpose of determining that Petitioner had not shown sufficiently that Exhibit 1027 was a printed publication and dismissed the Motion to Terminate as moot. Paper 23, 20.

[2] Peace Officer Background Investigation Tracking System ("POBITS").

Petitioner requested review by the Precedential Opinion Panel ("POP"). Req. 1; Ex. 3001. POP review was denied on June 16, 2020. Paper 26.

II. ANALYSIS

A. Legal Background

When rehearing a decision on institution, we review the decision for an abuse of discretion. *See* 37 C.F.R. § 42.71(c) (2019). An abuse of discretion may be indicated if a decision is based on an erroneous interpretation of law, if a factual finding is not supported by substantial evidence, or if the decision represents an unreasonable judgment in weighing relevant factors. *See Star Fruits S.N.C. v. U.S.*, 393 F.3d 1277, 1281 (Fed. Cir. 2005); *Arnold P'ship v. Dudas*, 362 F.3d 1338, 1340 (Fed. Cir. 2004); *In re Gartside*, 203 F.3d 1305, 1315–16 (Fed. Cir. 2000). The burden of showing that the Institution Decision should be modified is on Petitioner, the party challenging the Decision. *See* 37 C.F.R. § 42.71(d) (2019). In addition, "[t]he request must specifically identify all matters the party believes [we] misapprehended or overlooked, and the place where each matter was previously addressed in a motion, an opposition, or a reply." *Id.*

Whether a reference qualifies as a "printed publication" is a legal conclusion based on underlying factual findings. *See Nobel Biocare Servs. AG v. Instradent USA, Inc.*, 903 F.3d 1365, 1375 (Fed. Cir. 2018) (citing *Jazz Pharm., Inc. v. Amneal Pharm., LLC*, 895 F.3d 1347, 1356 (Fed. Cir. 2018)). The underlying factual findings include whether the reference was publicly accessible. *See id.* (citing *In re NTP, Inc.*, 654 F.3d 1279, 1296 (Fed. Cir. 2011)).

"The determination of whether a reference is a 'printed publication' under 35 U.S.C. § 102(b) involves a case-by-case inquiry into the facts and circumstances surrounding the reference's disclosure to members of the public." *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004). "Because there are many ways in which a reference may be disseminated to the interested public, 'public accessibility' has been called the touchstone in determining whether a reference constitutes a 'printed publication' bar under 35 U.S.C. § 102(b)." *Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1348 (Fed. Cir. 2016) (quoting *In re Hall*, 781 F.2d 897, 898–99 (Fed. Cir. 1986)). "A given reference is 'publicly accessible' upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art exercising reasonable diligence, can locate it." *SRI Int'l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc*., 445 F.3d 1374, 1378 (Fed. Cir. 2006)).

What constitutes a "printed publication" must be determined in light of the technology employed. *See* S*amsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1369 (Fed. Cir. 2019) (citing *In re Wyer*, 655 F.2d 221, 226 (CCPA 1981)). Public accessibility requires more than technical accessibility. *See id.* (citing *Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 773 (Fed. Cir. 2018)). "[A] work is not publicly accessible if the only people who know how to find it are the ones who created it." *Id.* at 1372. On the other hand, "a petitioner need not establish that specific persons actually accessed or received a work to show that the work was publicly accessible." *Id.* at 1374. "In fact, a limited distribution can make a work publicly accessible under certain circumstances."

Id. (quoting *GoPro, Inc. v. Contour IP Holding LLC*, 908 F.3d 690, 694 (Fed. Cir. 2018)).

"To prevail in a final written decision in an *inter partes* review, the petitioner bears the burden of establishing by a preponderance of the evidence that a particular document is a printed publication." *Hulu, LLC v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 11 (PTAB Dec. 20, 2019) (precedential). "[A]t the institution stage, the petition must identify, with particularity, evidence sufficient to establish a reasonable likelihood that the reference was publicly accessible before the critical date of the challenged patent and therefore that there is a reasonable likelihood that it qualifies as a printed publication." *Id.* at 13.

B. Printed Publication Status of Background Solutions and POBITS

For Background Solutions, Petitioner relied primarily on the third-party testimony of Tom Ward, the founder and co-owner of Background Solutions, LLC, to argue that Mr. Ward presented the Background Solutions video at national background investigation seminars and made the video available on a website, all prior to the critical date of the '188 patent. Pet. 18–24; Ex. 1009 (Ward Declaration). We found that Mr. Ward provided "vague and conclusory" testimony that lacked basic details such as "how many such seminars he presented at, when or where those seminars were, who attended the seminars, or who watched the 2009 Video at the seminars." Dec. 11–13. As to availability of Background Solutions on a website, we found that Petitioner's evidence, including Mr. Ward's testimony, did not show when Background Solutions was posted to the website, did not explain whether and how the website was indexed, and did

not provide any other information on how a skilled artisan would have located the reference. *Id.* at 13–17.

As to POBITS, Petitioner relied primarily on the third party testimony of Kingsley Klosson (Ex. 1014) and an Internet Archive capture (Ex. 1004) to argue that POBITS was available on an Internet website prior to the critical date of the '188 patent. Pet. 24. We found that, even if we credited Mr. Klosson's testimony, it did not allege enough facts to conclude that POBITS was publicly accessible. Dec. 17–19.

Petitioner's Request for Rehearing is based on four alleged mistakes: (1) we overlooked or misapprehended the standard for instituting an *inter partes* review when a petitioner relies on "non-traditional, electronic publications"; (2) we overlooked or misapprehended the difficulties involved in obtaining evidence from third parties at the institution stage; (3) because we did not resolve the parties' dispute as to the level of skill in the art, we misapprehended the significance of the third party witness testimony; and (4) we misapplied or misapprehended the level of proof necessary, at the institution stage, to show the public accessibility of a document on a public website. Req. 1–2.

1. Non-Traditional Electronic Publications and the Difficulties of Obtaining Third-Party Evidence

Petitioner's first two allegations, that we misapprehended the institution standard for non-traditional, electronic publications and the difficulties of obtaining third-party evidence pre-institution, are related. In short, Petitioner argues that we held its primary evidence of the public accessibility of Background Solutions and POBITS, third-party declarations, to an incorrectly high standard.

Petitioner contends that we did not recognize the "inherent difficulties" petitioners face in establishing the printed publication status of "non-traditional, electronic publications." Req. 3–4. Petitioner argues that *Hulu* addressed the "relative simplicity" of establishing a book housed in a library as publicly accessible but did not address the "added difficulties involved with non-traditional, electronic publications." *Id.* at 4–5 (citing *Hulu*, at 2–4). According to Petitioner, parties in its position face disadvantages such as the absence of hard copies on library shelves, lack of librarians ready to testify, and difficulties of obtaining the voluntary cooperation of third-party witnesses. *Id.* at 5–6. Petitioner argues that we abused our discretion by effectively holding Petitioner to a preponderance of the evidence standard at the institution stage. *Id.* at 6–7. Petitioner contends that its third-party witness testimony is "strong indicia" of public accessibility that meets the "totality of the evidence" standard set forth in *Hulu*. *Id.* at 7.

We are not persuaded. Although we are sympathetic to the difficulties a party might encounter in obtaining the cooperation of third parties while drafting a petition, the Statute and our Rules require a petitioner to set forth its case with particularity in the petition and to support that case with evidence. *See* 35 U.S.C. § 312(a)(3) ("A petition filed under section 311 may be considered only if— . . . (3) the petition identifies, in writing and *with particularity*, each claim challenged, the grounds on which the challenge to each claim is based, and *the evidence that supports the grounds for the challenge to each claim*, including— . . . (B) affidavits or declarations of supporting evidence . . . ." (emphasis added)); 37 C.F.R. § 42.104 (b). *Hulu* does not distinguish between "traditional" publications, such as books in a library, and "non-traditional" publications. In the case of

videos and websites, as well as books in a library, "at the institution stage, the petition must identify, with particularity, evidence sufficient to establish a reasonable likelihood that the reference was publicly accessible before the critical date of the challenged patent." *Hulu*, at 13. According to the *Hulu* panel, this "is a higher standard than mere notice pleading, but . . . it is lower than the 'preponderance' standard to prevail in a final written decision." *Id.* This is the standard to which we held Petitioner's evidence. Dec. 12–20.

It is the "particularity" required by *Hulu* that the Petition lacks. As we explained in the Decision, neither Petitioner nor Mr. Ward provided enough specificity to determine when Background Solutions was presented at seminars, when those seminars occurred, or who attended the seminars. Dec. 17. Thus, there is no persuasive evidence presented now from which we might later conclude that Background Solutions was publicly accessible by virtue of its display at seminars. Similarly, neither third-party witness provides any particularity as to how a skilled artisan would have located Background Solutions or POBITS on public websites. *Id.* at 17–19.

Petitioner contends that we "fail[ed] to recognize the serious differences" between developing a record at trial and making a showing in a Petition prior to institution. Req. 8. Petitioner argues that we should consider not only the evidence presented in the Petition but also evidence that may come out at trial. *Id.* at 8–9. Petitioner notes that the Board regularly grants motions to submit supplemental information under 37 C.F.R. § 42.123. *Id.* at 9. Indeed, *Hulu* recognizes that a petitioner may submit rebuttal evidence in a reply and move to submit supplemental information under Rule 42.123. *Hulu*, at 7–8. Petitioner argues that we erred by failing to consider what evidence Petitioner likely would have developed at trial. Req. 10.

As to the third-party declarations in particular, Petitioner's argument essentially is that it obtained the evidence that it could from Mr. Ward and Mr. Klosson and believes that they would provide more specific testimony if compelled during trial. Req. 10–12. As to Mr. Ward's testimony, Petitioner argues that, although "informed" by Petitioner's counsel, this testimony was produced voluntarily and uncompelled. *Id.* at 10. According to Petitioner, "Mr. Ward did not feel compelled to find, provide, or otherwise refresh his recollection about specific information requested by Guardian's counsel." *Id.* Petitioner argues that the same is true for Mr. Klosson's testimony. *Id.* at 11 ("The same argument applies to the Board's criticisms of Mr. Klosson's Declaration. He is a third party with no duty or obligation to incur the time or expense of voluntarily cooperating with Guardian.").

Petitioner misapprehends the role of rebuttal evidence and supplemental information. As *Hulu* notes, rebuttal evidence must respond to arguments raised by Patent Owner, rather than be evidence necessary to make Petitioner's prima facie case. *Hulu*, at 7 (citing 37 C.F.R. § 42.23). The evidence Petitioner presents in the Petition does not make a prima facie case of public accessibility. For example, Mr. Ward does not testify that he presented Background Solutions to anyone in any context prior to the critical date of the '188 patent. Even if we fully credit all of Mr. Ward's testimony, it is not sufficient to make Petitioner's prima facie case. Petitioner does not cite any authority for the proposition that it can simply allege public accessibility and later support those allegations with supplemental information adduced in a trial. That is akin to the "mere notice pleading" that *Hulu* confirms is insufficient for institution of a trial. *Hulu*, at 13.

Petitioner did not, in the Petition, present persuasive evidence that would lead us to believe that additional favorable evidence likely would be

uncovered through the discovery process. In fact, the Request confirms that the Petition presents no more than bare allegations of the public accessibility of Background Solutions and POBITS along with the hope that discovery in a trial would reveal evidence sufficient to prove those allegations. Pet. 19–24. For example, Petitioner "believes that once Mr. Ward and his company, Background Solutions, are compelled to gather and produce evidence, Mr. Ward will be able to specifically testify as to 'when or where the seminars occurred or who attended them' and the specific date by which the 2009 Video was posted on Background Solutions' website." Req. 11; *see also id.* ("The same argument applies to the Board's criticisms of Mr. Klosson's Declaration. He is a third party with no duty or obligation to incur the time or expense of voluntarily cooperating with [Petitioner]."). Yet, the Petition presents no persuasive evidence indicating what it expects to uncover and why. Petitioner's mere belief that Mr. Ward and Mr. Klosson will testify favorably in the future is more akin to notice pleading, rather than the "particularity" required by *Hulu*.

Thus, we did not apply an incorrect evidentiary standard at institution or misapprehend *Hulu*'s application to so-called "non-traditional" references.

2. Level of Skill in the Art

Petitioner argues that if we had resolved the level of skill correctly in our Decision, we would have concluded that the seminars at which Mr. Ward presented were attended by skilled artisans and, thus, that there is a reasonable likelihood that Background Solutions was publicly accessible. Req. 12–14.

In the Petition, citing to the Declarations of Mr. Ward and Mr. Klosson, Petitioner argued that a skilled artisan "would have had at least a high school degree, or equivalent thereof, and at least one to three years of experience in the relevant field, which includes background investigation methods, systems, and technologies." Pet. 5–6 (citing Exs. 1009, 1014). Petitioner argued that "Mr. Ward's presentation and demonstration of the Background Solutions video to a national conference of background investigators, i.e. those interested and skilled in the subject matter, qualifies it as a printed publication." *Id.* at 20–21. Patent Owner argued that "a police officer isn't the typical [person of ordinary skill in the art] that produces 'web based software applications,'" and that we should "adopt[] a level of skill appropriate for the software industry." Prelim. Resp. 7.[3] In the context of Background Solutions, we declined to resolve this dispute because Mr. Ward does not testify as to who attended the unidentified "law enforcement and background investigation seminars" at which he presented Background Solutions to "seminar attendees." Dec. 13 n.4; Ex. 1009 ¶¶ 7–9.

Petitioner argues that if we had resolved the level of skill in its favor, we would have understood the Declarations of Mr. Ward and Mr. Klosson differently (and more favorably to Petitioner). Req. 12–14. Specifically,

[3] Petitioner now states that "skilled artisans for the '188 patent include law enforcement officers (like Messrs. Ward, Klosson, and Miller)." Req. 14. It is unclear whether Petitioner is now advocating for a lower level of skill (law enforcement officers), or arguing that some law enforcement officers might have higher levels of skill (e.g., a law enforcement officer who also is a background investigator with at least one to three years of experience in background investigation methods, systems, and technologies). Pet. 5–6, 20–21; Req. 14.

Petitioner argues that "Mr. Ward's Declaration refers to 'law enforcement and background investigation seminars,' not general law enforcement seminars," and that Petitioner "understood Mr. Ward to be testifying that those attending the seminars where he presented the 2009 Video had backgrounds in law enforcement and/or background investigation." *Id.* at 12–13. According to Petitioner, we were misled by Patent Owner's arguments and, as a result, misunderstood that these seminars were no more than trade shows attended by police officers. *Id.* at 13 (citing Prelim. Resp. 7). Nevertheless, Petitioner argues, "[e]ven if the conferences were 'nothing more than trade shows,' [Petitioner] still believes that the evidence shows that police officers are skilled artisans in the context of the '188 patent." *Id.* Petitioner argues that if we "had at least considered [Petitioner's] position that skilled artisans for the '188 patent include law enforcement officers (like Messrs. Ward, Klosson, and Miller), then suddenly Mr. Ward's testimony about presenting the 2009 Video at seminars for law enforcement (as well as background investigators) becomes all the more complete." *Id.* at 14.

Petitioner misunderstands our determination. We did not implicitly adopt a level of skill requiring software industry experience and determine that only police officers attended the law enforcement and background investigation seminars at which Mr. Ward presented. We determined that the evidence did not support a finding that skilled artisans attended the seminars under any statement of the level of skill because Mr. Ward provided no information about who attended. Dec. 13 & n.4. Petitioner did not argue, in the Petition, that we should infer a level of skill of the attendees based on Mr. Ward's statement that he had presented at "law enforcement and background investigation seminars." Ex. 1009 ¶ 9. Thus, we could not

have overlooked such an argument. In any case, it would not have been persuasive, because Mr. Ward's vague statement does not imply any specific backgrounds for seminar attendees.

Moreover, even if Mr. Ward had been specific about the backgrounds of the attendees, he still did not testify that he presented at any seminar prior to the critical date of the '188 patent. Dec. 13. Thus, even if we were to accept Petitioner's new argument, Petitioner still has not presented sufficient evidence of public accessibility of Background Solutions.

3. Public Accessibility of a Document Posted to a Website

Petitioner contends that the 2010 copyright date on the face of POBITS, along with Mr. Klosson's testimony that he authored and uploaded POBITS onto his company's website by the end of 2010, is enough to show a reasonable likelihood that POBITS was publicly accessible prior to the critical date of the '188 patent. Req. 15. In the Decision, we determined that, even if we credit Mr. Klosson's testimony fully, simply showing that a reference was posted to an Internet website is not enough to show public accessibility by skilled artisans. Dec. 18–20 (citing *Blue Calypso*, 815 F.3d at 1349–50); *see also Samsung*, 929 F.3d at 1369 ("[W]hile indexing is not required to show that a work is publicly accessible, some evidence that a person of ordinary skill could have reasonably found the website and then found the reference on that website is critical.").

Petitioner now argues that MPEP[4] § 2128(II)(B) sets forth the standard for determining public accessibility of a document posted to a

[4] Manual of Patent Examining Procedure ("MPEP").

website. Req. 14–15. Petitioner did not make this argument in the Petition. Thus, we could not have overlooked it. Nevertheless, it is not persuasive.

MPEP § 2128(II)(B) provides: "Prior art disclosures on the Internet or on an online database are considered to be publicly available as of the date the item was publicly posted."[5] We discussed in the Decision, both for Background Solutions and POBITS, why, under Federal Circuit law, simply showing that a document was posted on the Internet is not sufficient to show that the document was publicly accessible. Dec. 13–20. We do not read the MPEP as inconsistent with Federal Circuit law. Indeed, MPEP § 2128(II)(B) expressly references § 2128(I), which makes clear that a reference is not shown to be publicly accessible in the absence of a showing that it was made available to the extent that skilled artisans, exercising reasonable diligence, could have located it. *See* MPEP § 2128(I) (citing *In re Wyer*, 655 F.2d 221 (CCPA 1981)); *see also* MPEP § 2128(II)(A) ("An electronic publication, including an online database or Internet publication (e.g., discussion group, forum, digital video, and social media post), is considered to be a 'printed publication' within the meaning of 35 U.S.C. 102(a)(1) and pre-AIA 35 U.S.C. 102(a) and (b) provided the publication was accessible to persons concerned with the art to which the document relates." (citing *Wyer*, 655 F.2d at 227)). Thus, MPEP § 2128(II)(B) provides guidance on the date a reference will be given during examination, provided that it is shown to be publicly accessible. It does not purport to provide the underlying standard for showing whether a reference was accessible to the relevant public.

[5] Petitioner appears to cite to the current version of the MPEP. However, the 8th edition, Revision 8, of MPEP § 2128, in force on April 6, 2012, provides similar discussion of public accessibility.

Petitioner also cites to several Board decisions that it contends contradict our institution decision. Req. 3–4, 14. Petitioner did not cite these cases in the Petition or argue their relevance. Pet. 18–24. Thus, we could not have misapprehended or overlooked them. In any case, these cases are non-precedential and were decided before *Hulu*. Our Decision considered Petitioner's evidence in light of the standards set forth in *Hulu* and Federal Circuit precedent. Petitioner does not persuade us that we misunderstood or misapplied the law.

III. CONCLUSION

For the foregoing reasons, Petitioner has not demonstrated that we misapprehended or overlooked its arguments or abused our discretion in denying the Petition.

IV. ORDER

In consideration of the foregoing, it is hereby:

ORDERED Petitioner's Request for Rehearing is *denied*.

FOR PETITIONER:

Jordan Sigale
Douglas Sorocco
DUNLAP CODDING, P.C.
jsigale@dunlapcodding.com
dsorocco@dunlapcodding.com

FOR PATENT OWNER:

Richard McLeod
MCLEOD LAW LLC
law@rickmcleod.com

Kurt Rylander
RYLANDER & ASSOCIATES PC
Rylander@rylanderlaw.com

Trials@uspto.gov
571.272.7822

Paper 26
Date: June 16, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

GUARDIAN ALLIANCE TECHNOLOGIES, INC.,
Petitioner,

v.

TYLER MILLER,
Patent Owner.

IPR2020-00031
Patent 10,043,188 B2

Before ANDREI IANCU, *Under Secretary of Commerce for Intellectual Property and Director of the United States Patent and Trademark Office*, ANDREW HIRSHFELD, *Commissioner for Patents*, and SCOTT R. BOALICK, *Chief Administrative Patent Judge.*

PER CURIAM.

ORDER

The Office has received a request for Precedential Opinion Panel (POP) review of an issue raised in this case. *See* Ex. 3001. The request was referred to the POP panel referenced above.

Upon consideration of the request, it is ORDERED that:

The request for POP review is denied; and

FURTHER ORDERED that the original panel maintains authority over all matters, including considering the submitted rehearing request.

For PETITIONER:

Jordan Sigale
jsigale@dunlapcodding.com

Douglas Sorocco
dsorocco@dunlapcodding.com

Evan Talley
etalley@dunlapcodding.com

For PATENT OWNER:

Richard McLeod
law@rickmcleod.com

Kurt Rylander
Rylander@rylanderlaw.com