The Steimel Law Group

Walter Steimel, Jr.
Principal

March 2, 2017

Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: **REQUEST FOR CONFIDENTIALITY PURSUANT TO 47 C.F.R. § 0.457(a), (c) and (d), 5 U.S.C. § 552(b)(4) AND 47 C.F.R. § 0.45 (Second Revised Letter)**

To Whom It May Concern:

On behalf of our client and Applicant, Locker LLC ("Locker"), we request long-term confidential treatment for certain information and documents, including but not limited to those identified below, which are part of the Part 90 Certification Application ("Application") submission made by UL on its behalf. We also request short-term confidential treatment of one hundred eighty (180) days for the Test Setup Photos, contained on pages 46 through 52 (inclusive) of the Certification Test Report. Please note that this is a revision to and amendment of both our original letter of November 8, 2016, and our revised letter of January 30, 2017.

Long-Term Confidentiality

Pursuant to 47 C.F.R. §§ 0.457 and 0.459, Locker requests that the Federal Communications Commission ("Commission") accord long-term confidential treatment to the majority of elements of its Application and the attachments to its Application. Locker is requesting long-term confidentiality because it will be divulging detailed information regarding the operation of its device, block diagrams, schematics and tuning instructions that detail the operation of the device. This information is confidential and proprietary and entitled to protection under the relevant statutes and rules. Keeping this information confidential is also essential to its central purpose. This device is unusual as it is used exclusively in anti-terrorism, security and law enforcement applications.

Locker's request for **Long-Term Confidentiality** includes all technical and operational descriptions. Locker's request includes, but is not limited to, the following items:

Descriptions of the device and operations
All internal photos
Block Diagrams and Schematics
Transceiver & Baseband Tuning Instructions
Antenna Specification

Operator's Manual (Users Manual)
Parts List
Tuning instructions
Operational description
Software and security information

Short-Term Confidentiality

The Test Setup Photos are also confidential and proprietary and entitled to protection under the relevant statutes and rules. Confidentiality is justified by the device's unique and unusual use in anti-terrorism, security and law enforcement applications. The Test Setup Photos contain some internal images of the device that would not be accessible without voiding the warranty and violating the terms of paragraph 1.2 of Locker's Confidentiality Agreement. In accordance with Commission practice, and for the reasons set forth herein, Locker requests **Short-Term Confidentiality** for the Test Setup Photos contained on pages 46 through 52 (inclusive) of the Certification Test Report.

Non-Confidential

Locker does not request confidentiality for the cover letter accompanying the Application; the attestation statements; this Confidentiality Request; the RF exposure information as this relates to operational safety; the external photos; the ID label or designation of its placement or the Test Report (with the exception of the Setup Photos, discussed above).

Application of Section 0.457(a) and (c)

The device in question is used in national security applications and covered by the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Parts 120-130. Access to information related to the device is generally restricted to those who acknowledge and certify that they will handle the information in accordance with applicable regulations and such information is generally not publicly available under the regulations. *See* 22 C.F.R. 126.10 and Subchapter R. Accordingly, Locker's submission should be withheld from public inspection pursuant to Section 0.457(a) and (c).

While these sections apply to all categories for which Locker seeks confidentiality, we provide further specific justification for three of these items. The Operator's Manual contains operational details that could compromise the effectiveness in using this device in anti-terrorism and law enforcement settings, and it is provided only under a Confidentiality Agreement, which Locker has provided to the Commission. The internal photos reveal details of the circuit board and components. Neither users nor the public are afforded access to view the circuit board or components. The device is kept and operated in screened and secure locations, and Locker requires all owners, operators and service technicians to execute the Confidentiality Agreement.

The Steimel Law Group
1455 Pennsylvania Avenue NW, Suite 770, Washington DC 20006
Telephone: 202-271-9258 E-mail: waltersteimel@gmail.com

Likewise, the Test Setup Photos reveal operational characteristics and test procedures that were researched and negotiated by Locker at significant expense, and contain images of the device with the back removed, revealing portions of the interior of the device. Competitors should not have the benefit of viewing the test setup that Locker devised for its device. While users of the device could, in the future, remove the back of the device (voiding the warranty and violating paragraph 1.2 of the Confidentiality Agreement), Locker deserves short-term confidentiality to protect it during its initial period of product rollout.

Application of Section 0.457(d)

In addition to the application of ITAR, details of Locker's device operation and performance characteristics constitute highly confidential trade secrets that the company has a right to keep from being disclosed to its competitors and the public at large. Much of the information provided in its Application constitutes either trade secrets or business proprietary information, the disclosure of which would subject Locker to significant competitive harm. Locker cannot afford to let its competitors know about its contemplation of entering the US market, the type of system or system configuration it is considering, or the designs, test analyses and engineering resolution of RF and similar matters. This information falls squarely within Section 0.457 (d), as further discussed below.

The instant request for confidentiality comports with the regulations and rulings of the Commission. The Commission has recognized that if disclosure of information submitted to the agency would result in competitive harm to the submitting party, the information must remain confidential. *Jeffrey A. Krause*, FOIA Control No. 96-80, MO&O, 11 FCC Rcd l0819 (l996) (*citing National Parks and Conservation Assn' v. Morton*, 498 F.2d 765, 770-71 (D.C. Cir. 1974)). In this instance examination of the information provided by Locker would permit competitors to design similar devices harming Locker's business.

In *The Matter of Checkpoint Systems, Inc*., 55 F.C.C.2d 268 (1975), Checkpoint requested access to applications for equipment authorization (certification) filed by Knogo for two field disturbance sensors and all supporting materials, equipment, and Commission requests. The Commission had previously determined that certain documents submitted in support of Knogo's certification applications were to be withheld from public inspection for a period of three years due to the fact that documents contained specific details (such as circuit parameter s and physical layouts) of a unique physical embodiment of the state of the art theory application used in the development of the equipment. This information was found to contain trade secrets warranting confidential treatment under the Commission's rules. The Commission believed that a competitor could take advantage of any technological advances made by Knogo and thereby cause injury to its competitive position. Checkpoint's application for review was denied in light of the determinations the Commission had previously made.

In *Michael R. Reynolds; On Request for Inspection of Records*, 89 FCC 2d 450 (1982),

The Steimel Law Group
1455 Pennsylvania Avenue NW, Suite 770, Washington DC 20006
Telephone: 202-271-9258 E-mail: waltersteimel@gmail.com

Reynolds sought access to the complete file of the approved subscription television system (STY) of American Television and Communications Corporation (ATC) for the purposes of writing a technical article about the system. The ATC application for approval of its system had been filed in November 1978 and confidentiality was granted for a period of 2 years with respect to those records concerning video signal coding and decoding and accompanying data contained in an application for a patent which at that time had not been granted. At the time of Reynolds' request, the two-year period of confidentiality had expired. However, the Chief Scientist notified ATC of the request for inspection. Subsequently, ATC requested extension of the original grant of confidentiality for an additional two-year term. The Commission granted ATC's extension and denied Reynolds' request for inspection in accordance with the Commission's policy to allow confidentiality for a limited period due to the fact that there had not been lengthy marketing of the device nor anything on the record to indicate that there had been public disclosure by ATC of any of the complex details of its encoding and decoding system and apparatus. To permit disclosure would, in effect, aid or assist those persons desirous of capitalizing on another's labor. Similarly, disclosure of Locker's information would permit third parties and competitors to benefit from Locker's labor.

In *Accounting Safeguards Under the Telecommunications Act of 1996*: Section 272(D) Biennial Audit Procedures. CC Docket No. 96- 150, FCC 02-239, 17 FCC Rcd 17102 (2002), the Commission discussed Rule 0.459 and set forth the showings that must be made to obtain confidential treatment. That case mentions three criteria that should be demonstrated - explanation of the substantial competitive harm, identification of measures to prevent disclosure and identification of previous disclosure to third parties.

In response to the criteria set forth in both the above-mentioned cases and Rules 0.457 and 0.459, Locker states that disclosure of the items disclosed to the Commission in its Application would expose Locker to substantial competitive harm by disclosing details of its competitive operational plans, and specifics of its design, operation and testing plan that are otherwise not public. Disclosure would enable competitors to determine Locker's design and engineering strategy, design, testing and operation details.

The data provided by Locker is specific raw data, and is not aggregated in any way to protect its confidentiality. Locker maintains extensive procedures to prevent the disclosure of all of this information, and it is not required to divulge this information otherwise. Locker does not divulge any aspect of its operations or products to third parties without strict confidentiality agreements (the Confidentiality Agreement) that it vigorously enforces. Locker has never made a public disclosure of this information, and has not disclosed this information to any third parties.

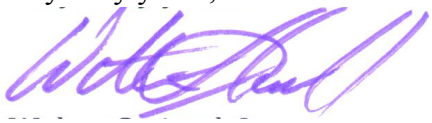
Locker also seeks non-disclosure of its activities with respect to its development and marketing of its devices. Not only is all of this information clearly confidential and proprietary under applicable precedent, it is particularly sensitive under the current circumstances.

The Steimel Law Group
1455 Pennsylvania Avenue NW, Suite 770, Washington DC 20006
Telephone: 202-271-9258 E-mail: waltersteimel@gmail.com

Locker has provided a sample of its Confidentiality Agreement. In addition, the operation of ITAR prohibits the dissemination of this information. To the extent that the Commission believes that the Confidentiality Agreement provisions need to be strengthened in order to support this request please notify us of that fact and we can make corresponding edits.

Should the Commission determine that any of the information submitted is not confidential, or desires to have Locker redact the written submission, Locker requests that the Commission provide it with time to undertake that effort. Locker requests that should the Commission deny this request for confidentiality, or should this information be subject to a requirement to make any of its filing public, that Locker be granted an opportunity to oppose such release, or withdraw its submission from the Commission. Locker should be granted the opportunity to seek a protective order should that prove to be necessary.

Very truly yours,



Walter Steimel, Jr.

CC: Locker, LLC
UL Verification Services Inc.

The Steimel Law Group
1455 Pennsylvania Avenue NW, Suite 770, Washington DC 20006
Telephone: 202-271-9258 E-mail: waltersteimel@gmail.com