UNITED STATES DISTRICT COURT

for the

Eastern District of Texas

Intertrust Technologies Corporation
Plaintiff
v.
Cinemark Holdings, Inc.
Defendant

Civil Action No. 2:19-cv-00266-JRG (Lead Case)

SUBPOENA TO PRODUCE DOCUMENTS, INFORMATION, OR OBJECTS OR TO PERMIT INSPECTION OF PREMISES IN A CIVIL ACTION

To: Dolby Laboratories, Inc.
1275 Market Street, San Francisco, CA 94103-1410
(Name of person to whom this subpoena is directed)

☑ *Production:* **YOU ARE COMMANDED** to produce at the time, date, and place set forth below the following documents, electronically stored information, or objects, and to permit inspection, copying, testing, or sampling of the material:

See Attachment A

Place:	Date and Time:
Quinn Emanuel Urquhart & Sullivan LLP 50 California St., 22nd Floor San Francisco, CA 94111	03/13/2020 9:00 am

☐ *Inspection of Premises:* **YOU ARE COMMANDED** to permit entry onto the designated premises, land, or other property possessed or controlled by you at the time, date, and location set forth below, so that the requesting party may inspect, measure, survey, photograph, test, or sample the property or any designated object or operation on it.

Place:	Date and Time:

The following provisions of Fed. R. Civ. P. 45 are attached – Rule 45(c), relating to the place of compliance; Rule 45(d), relating to your protection as a person subject to a subpoena; and Rule 45(e) and (g), relating to your duty to respond to this subpoena and the potential consequences of not doing so.

Date: 02/21/2020

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk | *Attorney's signature*

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Intertrust Technologies Corporation, who issues or requests this subpoena, are:

Richard Doss, 865 S. Figueroa Street, 10th floor, LA, CA 90017, richarddoss@quinnemanuel.com, (213) 443-3000

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things or the inspection of premises before trial, a notice and a copy of the subpoena must be served on each party in this case before it is served on the person to whom it is directed. Fed. R. Civ. P. 45(a)(4).

Civil Action No. 2:19-cv-00266-JRG (Lead Case)

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 45.)

I received this subpoena for *(name of individual and title, if any)* _____

on *(date)* _____ .

❒ I served the subpoena by delivering a copy to the named person as follows: _____

_____

_____ on *(date)* _____ ; or

❒ I returned the subpoena unexecuted because: _____

_____ .

Unless the subpoena was issued on behalf of the United States, or one of its officers or agents, I have also tendered to the witness the fees for one day's attendance, and the mileage allowed by law, in the amount of $ _____ .

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc.:

Federal Rule of Civil Procedure 45 (c), (d), (e), and (g) (Effective 12/1/13)

(c) Place of Compliance.

(1) ***For a Trial, Hearing, or Deposition.*** A subpoena may command a person to attend a trial, hearing, or deposition only as follows:

(A) within 100 miles of where the person resides, is employed, or regularly transacts business in person; or

(B) within the state where the person resides, is employed, or regularly transacts business in person, if the person

(i) is a party or a party's officer; or

(ii) is commanded to attend a trial and would not incur substantial expense.

(2) ***For Other Discovery.*** A subpoena may command:

(A) production of documents, electronically stored information, or tangible things at a place within 100 miles of where the person resides, is employed, or regularly transacts business in person; and

(B) inspection of premises at the premises to be inspected.

(d) Protecting a Person Subject to a Subpoena; Enforcement.

(1) ***Avoiding Undue Burden or Expense; Sanctions.*** A party or attorney responsible for issuing and serving a subpoena must take reasonable steps to avoid imposing undue burden or expense on a person subject to the subpoena. The court for the district where compliance is required must enforce this duty and impose an appropriate sanction—which may include lost earnings and reasonable attorney's fees—on a party or attorney who fails to comply.

(2) ***Command to Produce Materials or Permit Inspection.***

(A) *Appearance Not Required.* A person commanded to produce documents, electronically stored information, or tangible things, or to permit the inspection of premises, need not appear in person at the place of production or inspection unless also commanded to appear for a deposition, hearing, or trial.

(B) *Objections.* A person commanded to produce documents or tangible things or to permit inspection may serve on the party or attorney designated in the subpoena a written objection to inspecting, copying, testing, or sampling any or all of the materials or to inspecting the premises—or to producing electronically stored information in the form or forms requested. The objection must be served before the earlier of the time specified for compliance or 14 days after the subpoena is served. If an objection is made, the following rules apply:

(i) At any time, on notice to the commanded person, the serving party may move the court for the district where compliance is required for an order compelling production or inspection.

(ii) These acts may be required only as directed in the order, and the order must protect a person who is neither a party nor a party's officer from significant expense resulting from compliance.

(3) ***Quashing or Modifying a Subpoena.***

(A) *When Required.* On timely motion, the court for the district where compliance is required must quash or modify a subpoena that:

(i) fails to allow a reasonable time to comply;

(ii) requires a person to comply beyond the geographical limits specified in Rule 45(c);

(iii) requires disclosure of privileged or other protected matter, if no exception or waiver applies; or

(iv) subjects a person to undue burden.

(B) *When Permitted.* To protect a person subject to or affected by a subpoena, the court for the district where compliance is required may, on motion, quash or modify the subpoena if it requires:

(i) disclosing a trade secret or other confidential research, development, or commercial information; or

(ii) disclosing an unretained expert's opinion or information that does not describe specific occurrences in dispute and results from the expert's study that was not requested by a party.

(C) *Specifying Conditions as an Alternative.* In the circumstances described in Rule 45(d)(3)(B), the court may, instead of quashing or modifying a subpoena, order appearance or production under specified conditions if the serving party:

(i) shows a substantial need for the testimony or material that cannot be otherwise met without undue hardship; and

(ii) ensures that the subpoenaed person will be reasonably compensated.

(e) Duties in Responding to a Subpoena.

(1) ***Producing Documents or Electronically Stored Information.*** These procedures apply to producing documents or electronically stored information:

(A) *Documents.* A person responding to a subpoena to produce documents must produce them as they are kept in the ordinary course of business or must organize and label them to correspond to the categories in the demand.

(B) *Form for Producing Electronically Stored Information Not Specified.* If a subpoena does not specify a form for producing electronically stored information, the person responding must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms.

(C) *Electronically Stored Information Produced in Only One Form.* The person responding need not produce the same electronically stored information in more than one form.

(D) *Inaccessible Electronically Stored Information.* The person responding need not provide discovery of electronically stored information from sources that the person identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the person responding must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

(2) ***Claiming Privilege or Protection.***

(A) *Information Withheld.* A person withholding subpoenaed information under a claim that it is privileged or subject to protection as trial-preparation material must:

(i) expressly make the claim; and

(ii) describe the nature of the withheld documents, communications, or tangible things in a manner that, without revealing information itself privileged or protected, will enable the parties to assess the claim.

(B) *Information Produced.* If information produced in response to a subpoena is subject to a claim of privilege or of protection as trial-preparation material, the person making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information under seal to the court for the district where compliance is required for a determination of the claim. The person who produced the information must preserve the information until the claim is resolved.

(g) Contempt.

The court for the district where compliance is required—and also, after a motion is transferred, the issuing court—may hold in contempt a person who, having been served, fails without adequate excuse to obey the subpoena or an order related to it.

For access to subpoena materials, see Fed. R. Civ. P. 45(a) Committee Note (2013).

ATTACHMENT A

ATTACHMENT A TO DOCUMENT SUBPOENA

Pursuant to Rule 45 of the Federal Rules of Civil Procedure, Plaintiff Intertrust Technologies Corporation hereby requests that Dolby Laboratories, Inc. produce and permit inspection and copying of the following documents and things at the place, date and time specified in the accompanying subpoena.

DEFINITIONS

The following definitions are to be used for purposes of responding to this subpoena:

1. The term "You," "Your," or "Dolby" should be understood to refer to Dolby Laboratories, Inc., including without limitation all corporate locations, as well as any officers, directors, partners, associates, employees, staff members, agents, representatives, attorneys, consultants, subsidiaries foreign or domestic, parents, affiliates, divisions, successors, predecessors, and any others acting or purporting to act for you or on your behalf.

2. The term "Intertrust" is defined as Intertrust Technologies Corporation, and should be understood to include any and all officers, directors, partners, associates, employees, staff members, agents, representatives, attorneys, subsidiaries, parents, affiliates, divisions, successors, predecessors, or other related entities.

3. The term "Defendant" should be understood to include Cinemark Holdings, Inc., AMC Entertainment Holdings, Inc., and Regal Entertainment Group, individually. "Defendant" is intended to be interpreted in the manner that leads to the broadest scope of documents responsive to the category in which the term appears and should be understood to include any officers, directors, partners, associates, employees, staff members, agents, representatives, attorneys, consultants, subsidiaries foreign or domestic, parents, affiliates, divisions, successors, predecessors, and any others acting on behalf of a Defendant or under a Defendant's direction and

control, and any and all assets or entities that have been acquired by a Defendant or to which a Defendant has succeeded to rights or obligations.

4. The term "document" is defined as synonymous in meaning and equal in scope to the usage of this term in Federal Rule of Civil Procedure 34(a), and should be understood to include any written, printed, typed, and visually, aurally, or electronically reproduced material of any kind, whether or not privileged, including but not limited to electronic mail, computer files, source code, backup media, and databases; files and file folders; books and their contents, whether printed or recorded or reproduced by hand or any other mechanical process, or written or reproduced by hand or any other mechanical process; and all other tangible manifestations of communications whether or not claimed to be privileged, confidential, or personal; namely, communications, including intra-company communications, correspondence, telegrams, memoranda, summaries or records of telephone conversations, summaries or records of personal conversations; diaries; forecasts; statistical statements; laboratory and engineering reports and notebooks, changes, plans, specifications, data sheets, drawings, schematics, graphs, flow charts, samples, prototypes and tangible things, evaluation boards, developers guidelines; photographs, films, pictures, and videotapes; minutes or records of meetings, including directors' meetings, minutes or records of conferences; expressions of statements or policy; lists of persons attending meetings or conferences; reports and/or summaries of interviews or investigations; opinions or reports of consultants' patent appraisals; opinions of counsel; agreements; records, reports or summaries of negotiations; brochures, pamphlets, advertisements, circulars, trade letters, packing materials and notices, press releases; litigation files and databases; and any drafts or revisions of any document and any notes or comments appearing on any document, whether preliminary or marginal. A comment or notation appearing on any document, and not a part of the original document, is

considered a separate document within the meaning of the term. A draft or non-identical copy is a separate document within the meaning of the term.

5. The term "communication" should be understood to include all inquiries, discussions, conversations, negotiations, agreements, understandings, meetings, telephone conversations, letters, facsimiles, notes, telegrams, emails, advertisements, or other forms of verbal exchange, whether oral or written.

6. The term "product" should be understood to include any product, device, apparatus, process, system, service, software, or instrumentality.

7. The term "Content" should be understood to mean any digital image, audio, caption, or subtitle information, including any associated metadata, that forms part of a feature film, short film, advertisement, trailer, or logo.

8. The term "DCI Specification" refers to the Digital Cinema System Specification, including Versions 1.0, 1.1, 1.2, and 1.3, along with all Errata thereto, and/or any earlier or later versions along with Errata thereto. For reference, attached hereto are Version 1.2 with Errata as of 30 August 2012 Incorporated, published by Digital Cinema Initiatives, LLC ("DCSS v1.2")[1] as modified by Erratum # 9 (Chapter 9 Replacement) to the DCSS v1.2.[2]

9. The term "DCI-compliant Equipment" should be understood to mean any product, process, component, system, service, software, instrumentality, or equipment that is or is alleged to be compliant with the DCI Specification or any product, process, component, system, service, software, instrumentality, or equipment that works, interfaces, or communicates with other products, processes, components, systems, services, software, instrumentalities, or equipment that

[1] DCSS v1.2 is Attachment B to this subpoena.
[2] Erratum # 9 to the DCSS v1.2 is Attachment C to this subpoena.

are or are alleged to be compliant with the DCI Specification, including, but not limited to, any such product, process, component, system, service, software, instrumentality, or equipment that has been certified as being compliant with the DCI Specification. Some non-limiting, non-exclusive examples of DCI-compliant Equipment include SMSs, TMSs, Media Blocks, SPBs, storage devices, and digital projectors described in the DCI Specification.

10. The term "Security Manager" refers to the Security Manager(s) defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Security Manager(s) therein.

11. The term "Media Decryptor" refers to the Media Decryptor defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Media Decryptor therein.

12. The term "Secure Processing Block" or "SPB" refers to any of the Secure Processing Blocks defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the corresponding Secure Processing Block therein.

13. The term "Security Entities" refers to any of the Security Entities defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to Security Entities therein.

14. The term "Key Delivery Message" or "KDM" refers to the Key Delivery Message described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Key Delivery Message therein.

15. The term "Media Block" refers to the Image Media Block and the Outboard Media Block defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to each therein.

16. The term "Trusted Device List" or "TDL" refers to the Trusted Device List defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Trusted Device List therein.

17. The term "Screen Management System" or "SMS" refers to the Screen Management System defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Screen Management System therein.

18. The term "Theater Management System" or "TMS" refers to the Theater Management System defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Theater Management System therein.

19. The term "Composition Playlist" or "CPL" refers to the Composition Playlist defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Composition Playlist therein.

20. The term "Forensic Marker" refers to the Forensic Marker defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Forensic Marker therein.

21. The term "Link Encryptor" or "LE" refers to the Link Encryptor defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Link Encryptor therein.

22. The term "Link Decryptor" or "LD" refers to the Link Decryptor defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Link Decryptor therein.

23. The term "Link Decryptor Block" or "LDB" refers to the Link Decryptor Block defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Link Decryptor Block therein.

24. The term "Digital Cinema Package" or "DCP" refers to the Digital Cinema Package defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Digital Cinema Package therein.

25. The term "Track Files" refers to the Track Files defined and described in the DCI Specification including all of the functions, requirements, properties, characteristics, and components ascribed to the Track Files therein.

26. "Supplied Equipment" shall mean all DCI-compliant Equipment provided by you, in whole or in part, to any Defendant, or to any third party for use in products or services to be provided to any Defendant, including but not limited to all versions of the Dolby Digital Cinema Server DSS100, Dolby Digital Cinema Server DSS200, Dolby Digital Cinema Server DSP100, Dolby DSL 100, Dolby Cat. No. 745 Integrated Media Server, Dolby Cat. No. 862 Integrated Media Server, Dolby/Doremi Integrated Media Server IMS1000, Dolby Integrated Media Server IMS2000, Dolby Integrated Media Server IMS3000, Doremi Cinema Integrated Media Server ShowVault, Doremi Digital Cinema Server DCP-2000, Doremi Digital Cinema Server DCP-2000-NTS, Doremi Digital Cinema Server Montage CDCS 2000, and Doremi Digital Cinema Server DCP-2K4.

27. The phrase "the '721 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 6,157,721,[3] including but not limited to, all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in receiving software or firmware, or any updates thereto, that is executable by a Media Block or other SPBs; and all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in obtaining and authenticating a digital signature and/or certificate associated with software or firmware, or any updates thereto, that is executable by a Media Block or other SPBs including any related data, such as licenses, authorization, and/or authentication objects and their schemas associated with installation or use of the Supplied Equipment.

28. The phrase "the '304 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 6,640,304,[4] including but not limited to, all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy

[3] *See* '721 Patent claim chart included as Attachment D to this subpoena.
[4] *See* '304 Patent claim chart included as Attachment E to this subpoena.

the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving encrypted Content, such as a Digital Cinema Package and/or encrypted track files, (b) receiving and authenticating a KDM, (c) checking whether all KDM conditions are satisfied, including determining that each SPB, including a Media Block hosting a Security Manager, has a valid certificate on a TDL associated with a KDM, and enabling playback only for a start time within the authorized time window for playback specified in a KDM, (d) collecting and storing log information from remote SPBs and generating and sending log reports, (e) monitoring and logging integrity status of a Media Block and remote Secure Processing Blocks, (f) determining that a Media Block or remote SPB has not been tampered with, and (g) terminating functionalities or deleting data, such as private keys, content keys, content integrity keys, or other cryptographic data, in response to determining that a Media Block or SPB has been tampered with.

29. The phrase "the '815 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 6,785,815,[5] including but not limited to, all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving a request, for example at an SMS or TMS, from an operator to start or stop playback of Content, (b) sending a request from an SMS or TMS to a Security Manager to start or stop playback of Content, (c) receiving or ingesting encrypted Content, such as, but not limited to, Digital Cinema

[5] *See* '815 Patent claim chart included as Attachment F to this subpoena.

Packages and encrypted Track Files, (d) receiving or ingesting a Composition Playlist including a digital signature and hashes of Track Files, (e) receiving HMAC values associated with the Track Files, (f) processing Track File integrity pack metadata during playback, and logging any integrity pack deviations (including HMAC) detected, (g) receiving and authenticating a KDM, (h) authenticating a Composition Playlist, (i) authenticating the integrity of Track Files using hashes of Track Files received as part of a Composition Playlist, and (j) enabling playback of Content consistent with Composition Playlist.

30. The phrase "the '602 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 7,340,602,[6] including but not limited to, all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) collecting and storing log information from remote Secure Processing Blocks, (b) generating log reports, and (c) exporting log reports.

31. The phrase "the '603 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 7,406,603,[7] including but not limited to, all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy

[6] *See* '602 Patent claim chart included as Attachment G to this subpoena.
[7] *See* '603 Patent claim chart included as Attachment H to this subpoena.

the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving a request to playback, access, or process Content, (b) monitoring downstream SPBs and Security Entities involved in media decryption, forensic marking, or link encryption/decryption to determine that Content is directed only to trusted SPBs and Security Entities, (c) receiving and authenticating a KDM, (d) obtaining encrypted content keys from a KDM, (e) decrypting encrypted content keys received from a KDM, (f) checking whether all Security Entities are valid and KDM conditions are satisfied, (g) sending decrypted content keys to a Media Decryptor, (h) determining that a Media Block hosting a Security Manager has not been tampered with, (i) determining that each SPB, including a Media Block hosting a Security Manager, has a valid certificate on the Trusted Device List associated with the KDM, (j) terminating functionalities or deleting data, such as private keys, content keys, content integrity keys, or other cryptographic data, in response to determining that a Media Block hosting a Security Manager has been tampered with, (k) generating and providing link encryption/decryption keys to a Link Encryptor and Link Decryptor, (l) receiving instructions at a Media Decryptor to decrypt encrypted Content, (m) receiving decrypted content keys at a Media Decryptor, (n) decrypting encrypted Content at a Media Decryptor using content keys, (o) generating and inserting forensic markers in real-time (e.g., during Content playback) into Content, (p) receiving Content at a Link Encryptor, (q) receiving cryptographic keys at a Link Encryptor, (r) encrypting Content received at a Link Encryptor using cryptographic keys, (s) transmitting encrypted Content from a Link Encryptor to a Link Decryptor Block, (t) receiving a request at an SMS or TMS from an operator

to start or stop playback of Content, and (u) sending a request to a Security Manager to start or stop playback of Content.

32. The phrase "the '342 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 7,694,342,[8] including but not limited to, all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) authenticating remote SPBs and SMSs by establishing Transport Layer Security (TLS) sessions, (b) determining that each SPB, including the Media Block hosting the Security Manager, has a valid certificate on a TDL associated with the KDM, (c) receiving a request to playback, access, or process Content, (d) receiving and authenticating a KDM associated with Content, (e) obtaining and decrypting encrypted content keys from a KDM, (f) checking whether all Security Entities are valid and KDM conditions are satisfied, (g) monitoring downstream SPBs and Security Entities involved in media decryption, forensic marking, or link encryption/decryption to determine that Content is directed only to trusted SPBs and Security Entities, (h) receiving and authenticating a Composition Playlist, (i) validating that a KDM is associated with a Composition Playlist, (j) determining that the Media Block hosting a Security Manager has not been tampered with, (k) monitoring and logging integrity status of a Media Block and remote Secure Processing

[8] *See* '342 Patent claim chart included as Attachment I to this subpoena.

Blocks, (l) terminating functionalities or deleting data, such as private keys, content keys, content integrity keys, or other cryptographic data, in response to determining that a Media Block hosting a Security Manager has been tampered with, (m) receiving a request at an SMS or TMS from an operator to start or stop playback of Content, and (n) sending a request from the SMS or TMS to the Security Manager to start or stop playback of Content.

33. The phrase "the '157 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 8,191,157,[9] including but not limited to, all versions of all components providing execution of software or firmware instructions that are incorporated into any of the Supplied Equipment, including any processors, CPUs, microprocessors, microcontrollers, FPGAs, ASICs, or DSPs; all versions of all components providing volatile or nonvolatile memory or storage that are incorporated into any of the Supplied Equipment, including any Random Access Memory (RAM), hard-drive storage, solid-state or flash-drive storage; all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving or ingesting encrypted Content, such as, but not limited to, Digital Cinema Packages and encrypted Track Files, Composition Playlists, and Key Delivery Messages, (b) storing encrypted Content, such as, but not limited to Digital Cinema Packages and

[9] *See* '157 Patent claim chart included as Attachment J to this subpoena.

encrypted Track Files, Composition Playlists, and Key Delivery Messages, (c) receiving a request to playback, access, or process Content, (d) instructing a Media Decryptor to decrypt encrypted Content, (e) monitoring downstream Secure Processing Blocks and Security Entities involved in media decryption, forensic marking, or link encryption/decryption, (f) storing cryptographic private, public, or symmetric keys, (g) receiving and authenticating a KDM, (h) obtaining and decrypting encrypted content keys from a KDM, (i) checking whether all Security Entities are valid and KDM conditions are satisfied, (j) sending decrypted content keys to a Media Decryptor, (k) determining that a Media Decryptor is of the type corresponding to a key type ID designated by a KDM, (l) determining that a Media Decryptor is authorized to receive decrypted content keys to decrypt encrypted Content, (m) determining that a Media Block hosting a Security Manager has not been tampered with, (n) determining that each SPB, including a Media Block hosting a Security Manager, has a valid certificate on a Trusted Device List associated with a KDM, (o) terminating functionalities or deleting data, such as private keys, content keys, content integrity keys, or other cryptographic data, in response to determining that a Media Block hosting a Security Manager has been tampered with, (p) authenticating a Composition Playlist, (q) validating that a KDM is associated with a Composition Playlist, (r) generating and providing link encryption/decryption keys to a Link Encryptor and Link Decryptor, (s) receiving instructions at a Media Decryptor to decrypt encrypted Content, (t) receiving decrypted content keys at a Media Decryptor, (u) decrypting encrypted Content at a Media Decryptor using content keys, (v) receiving Content at a Link Encryptor, (w) receiving cryptographic keys at a Link Encryptor, (x) encrypting Content received at a Link Encryptor using cryptographic keys, (y) transmitting encrypted Content from a Link Encryptor to a Link Decryptor Block, (z) receiving encrypted Content at a Link Decryptor, (aa) receiving cryptographic keys at a Link Decryptor, (bb) decrypting encrypted Content received

at a Link Decryptor using cryptographic keys, (cc) providing unencrypted Content from a Link Decryptor to a projector SPB; (dd) receiving a request at an SMS or TMS from an operator to start or stop playback of Content, and (ee) sending a request from an SMS or TMS to a Security Manager to start or stop playback of Content.

34. The phrase "the '158 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 8,191,158,[10] including but not limited to, all versions of all components providing execution of software or firmware instructions that are incorporated into any of the Supplied Equipment, including any processors, CPUs, microprocessors, microcontrollers, FPGAs, ASICs, or DSPs; all versions of all components providing volatile or nonvolatile memory or storage that are incorporated into any of the Supplied Equipment, including any Random Access Memory (RAM), hard-drive storage, solid-state or flash-drive storage; all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving or ingesting encrypted Content, such as, but not limited to, Digital Cinema Packages and encrypted Track Files, Composition Playlists, and Key Delivery Messages, (b) storing encrypted Content, such as, but not limited to Digital Cinema Packages and encrypted Track Files, Composition Playlists, and Key Delivery Messages, (c) receiving a request

[10] *See* '158 Patent claim chart included as Attachment K to this subpoena.

to playback, access, or process Content, (d) instructing a Media Decryptor to decrypt encrypted Content, (e) monitoring downstream SPBs and Security Entities involved in media decryption, forensic marking, or link encryption/decryption, (f) storing cryptographic private, public, or symmetric keys, (g) receiving and authenticating a KDM, (h) obtaining and decrypting encrypted content keys from a KDM, (i) checking whether all Security Entities are valid and KDM conditions are satisfied, (j) determining that a Media Block hosting a Security Manager has not been tampered with, (k) determining that each SPB, including a Media Block hosting a Security Manager, has a valid certificate on the Trusted Device List associated with a KDM, (l) receiving instructions at a Media Decryptor to decrypt encrypted Content, (m) receiving decrypted content keys at a Media Decryptor, (n) decrypting encrypted Content at a Media Decryptor using content keys, (o) receiving a request at an SMS or TMS from an operator to start or stop playback of Content, and (p) sending a request from an SMS or TMS to a Security Manager to start or stop playback of Content.

35. The phrase "the '106 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 8,931,106,[11] including but not limited to, all versions of all components providing execution of software or firmware instructions that are incorporated into any of the Supplied Equipment, including any processors, CPUs, microprocessors, microcontrollers, FPGAs, ASICs, or DSPs; all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy the requirements of Federal

[11] *See* '106 Patent claim chart included as Attachment L to this subpoena.

Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving or ingesting encrypted Content, such as, but not limited to, Digital Cinema Packages and encrypted Track Files, Composition Playlists, and Key Delivery Messages, (b) receiving a request to playback, access, or process Content, (c) instructing a Media Decryptor to decrypt encrypted Content, (d) monitoring downstream Secure Processing Blocks and Security Entities involved in media decryption, forensic marking, or link encryption/decryption, (e) receiving and authenticating a KDM, (f) obtaining and decrypting encrypted content keys from a KDM, (g) checking whether all Security Entities are valid and KDM conditions are satisfied, (h) determining that a Media Block hosting a Security Manager has not been tampered with, (i) determining that each SPB, including a Media Block hosting a Security Manager, has a valid certificate on the Trusted Device List (TDL) associated with a KDM, (j) receiving instructions at a Media Decryptor to decrypt encrypted Content, (k) receiving decrypted content keys at a Media Decryptor, and (l) decrypting encrypted Content at a Media Decryptor using content keys.

36. The phrase "the '627 Patent Accused Functionalities" shall mean all components, functionalities, and technologies of each Supplied Equipment consistent with the Accused Instrumentalities identified in Intertrust's P.R. 3-1 Disclosure (including any amendments and supplements thereto) as infringing U.S. Patent No. 9,569,627,[12] including but not limited to, all versions of all components providing execution of software or firmware instructions that are incorporated into any of the Supplied Equipment, including any processors, CPUs, microprocessors, microcontrollers, FPGAs, ASICs, or DSPs; all versions of all components

[12] *See* '627 Patent claim chart included as Attachment M to this subpoena.

providing volatile or nonvolatile memory or storage that are incorporated into any of the Supplied Equipment, including any Random Access Memory (RAM), hard-drive storage, solid-state or flash-drive storage; all software, firmware or hardware incorporated into any of the Supplied Equipment that is in any way involved in providing any aspect of the Supplied Equipment with security features that satisfy the requirements of Federal Information Processing Standards (FIPS) 140-2 Level 3 in any areas; all software, firmware or hardware incorporated into any of the Supplied Equipment that is involved in any of the functions performed by the Supplied Equipment, such as, but not limited to, (a) receiving a request to playback, access, or process Content, (b) instructing a Media Decryptor to decrypt encrypted Content, (c) monitoring downstream Secure Processing Blocks and Security Entities involved in media decryption, forensic marking, or link encryption/decryption, (d) storing cryptographic private, public, or symmetric keys, (e) receiving and authenticating a KDM, (f) obtaining encrypted content keys from the KDM, (g) decrypting encrypted content keys received from a KDM, (h) checking whether all Security Entities are valid and KDM conditions are satisfied, (i) checking whether logging sub-system(s) are operative, (j) sending decrypted content keys to the Media Decryptor, (k) determining that Media Decryptor is of the type corresponding to a key type ID designated by a KDM, (l) determining that the Media Decryptor is authorized to receive decrypted content keys to decrypt encrypted Content, (m) determining that the Media Block hosting the Security Manager has not been tampered with, (n) determining that each SPB, including the Media Block hosting the Security Manager, has a valid certificate on the Trusted Device List (TDL) associated with the KDM, (o) terminating functionalities or deleting data, such as private keys, content keys, content integrity keys, or other cryptographic data, in response to determining that the Media Block hosting the Security Manager has been tampered with, (p) receiving instructions at a Media Decryptor to decrypt encrypted

Content, (q) receiving decrypted content keys at a Media Decryptor, (r) decrypting encrypted Content at a Media Decryptor using content keys, (s) receiving a request at an SMS or TMS from an operator to start or stop playback of Content, (t) sending a request from an SMS or TMS to a Security Manager to start or stop playback of Content, and (u) sending a request to the Security Manager to instruct the Media Decryptor to decrypt encrypted Content.

37. The phrase "Accused Functionalities" shall mean all of the '721 Patent Accused Functionalities, the '304 Patent Accused Functionalities, the '815 Patent Accused Functionalities, the '602 Patent Accused Functionalities, the '603 Patent Accused Functionalities, the '342 Patent Accused Functionalities, the '157 Patent Accused Functionalities, the '158 Patent Accused Functionalities, the '106 Patent Accused Functionalities, and the '627 Patent Accused Functionalities identified above in paragraphs 27 through 36.

38. The term "person" should be understood to include any natural person or any corporate, business, legal, or governmental entity or association.

39. The terms "relate to," "related to," "in relation to" and "relating to" stated subject matter should be understood to include any and all communications or documents that bear upon, constitute, contain, embody, evidence, comprise, reflect, identify, pertain to, state, comment on, respond to, describe, analyze, or are in any way relevant to that subject matter, whether directly or indirectly or in whole or in part, including without limitation documents related to the subject of inquiry or the existence of other documents relating to the subject.

40. The term "including" is defined as "including, without limitation."

41. The term "each" is defined as including "every," and the term "every" is defined as including "each."

42. The term "any" is defined as including "all," and the term "all" is defined as including "every."

43. The disjunctive shall be construed as the conjunctive, and the conjunctive shall be construed as the disjunctive, and the connectives "and" and "or" shall be construed disjunctively or conjunctively as necessary to bring within the scope of these requests all responses that might otherwise be construed to be outside of their scope.

44. The use of a verb in any tense shall be construed as the use of that verb in all other tenses necessary to bring within the scope of these requests all responses that might otherwise be construed to be outside of their scope.

45. A plural noun shall be construed as a singular noun, and a singular noun shall be construed as a plural noun, as necessary to bring within the scope of these requests all responses that might otherwise be construed to be outside of their scope.

46. The term “Case” is defined as Intertrust’s Complaints and/or counterclaims filed in the Eastern District of Texas, Case Nos. 2:19-cv-00266-JRG (Lead Case), 2:19-cv-00265-JRG, and 2:19-cv-00267-JRG, and should be understood to include any and all amended complaint(s) as of the date that such amended version is filed with the Court.

47. The term “Asserted Patents” is defined as the patents asserted by Intertrust in its Complaints in this litigation, including U.S. Patent No. 6,157,721 (“the ’721 Patent”), U.S. Patent No. 6,640,304 (“the ’304 Patent”), U.S. Patent No. 6,785,815 (“the ’815 Patent”), U.S. Patent No. 7,340,602 (“the ’602 Patent”), U.S. Patent No. 7,406,603 (“the ’603 Patent”), U.S. Patent No. 7,694,342 (“the ’342 Patent”), U.S. Patent No. 8,191,157 (“the ’157 Patent”), U.S. Patent No. 8,191,158 (“the ’158 Patent”), U.S. Patent No. 8,931,106 (“the ’106 Patent”), and U.S. Patent No. 9,569,627 (“the ’627 Patent”). Any additional patent or patents asserted by Intertrust in any

amended version(s) of the complaint are within the meaning of the term as of the date that such amended version is filed with the Court.

48. The term “Asserted Claims” is defined as the claims of the Asserted Patents that Intertrust identified as infringed in its infringement contentions. Any additional claims identified by Intertrust in any amended version(s) of its infringement contentions are within the meaning of the term as of the date that such amended version is served.

49. "Source Code" means computer code that specifies software that executes on processors (including but not limited to CPUs, embedded processors, DSPs, microcontrollers, FPGAs) of the Supplied Components, or on processors of a Defendant's computer or server (including but not limited to code written in the C, C++, C#, Objective C, Visual Basic, Java, JavaScript, PHP programming languages, in assembly language, in mark-up languages such as HTML or XML, or in data object formats such as JSON), or hardware definition/design language code that specifies the structure or functionality of hardware logic (including but not limited to code written in the Verilog or VHDL languages).

INSTRUCTIONS

1. In responding to these requests, you are required to furnish all documents available to you including, but not limited to, information in the possession or control of your attorneys, experts, advisers, agents, associates or any other person over whom you have control.

2. You are requested to produce all documents and things in the following categories that are in your possession, custody or control, in their entirety and without redaction or expurgation. "Possession, custody or control" shall be construed to the fullest extent provided under Federal Rules of Civil Procedure 26, 34 and 45 and shall include, without limitation, those

documents and things in the hands of any other person that you have the ability to demand or to gain access to in the ordinary course of business.

3. With respect to any information responsive to these requests that is electronically stored, you are required to ensure that such information is preserved in its original native format from the date that the subpoena is served through the latest end date of any of the Cases, whether terminated by settlement, dismissal (with or without prejudice) or actual court decision. You are required to produce all electronically stored information in the format in which such information was created or is presently stored. If you are unable to produce such information in its native electronic format, then you shall promptly advise counsel for Intertrust identified on the subpoena to which this Attachment A is attached, and seek to reach mutual agreement on the format for production of such information.

4. If any document is withheld based upon a claim of privilege or other protection, provide for each such document: (i) the date of the document, (ii) the names of all authors of the document, (iii) the names of all recipients of the document, (iv) the names of all cc and/or bcc recipients of the document, (v) the type of document, (vi) a description of the document, (vii) an identification of the privilege or protection claimed, and (viii) a brief explanation of the basis of your claim of privilege or other protection.

5. Documents shall not be withheld on the grounds that they contain highly sensitive or confidential information, but instead shall be designated in accordance with the terms of the Protective Order entered by the Court in the Case and provided as Attachment N to this subpoena.

DOCUMENTS REQUESTED

1. All documents that constitute, refer to or relate to, any software, computer code, programs, or hardware used to operate, enable, or implement any Accused Functionalities of the Supplied Equipment, including but not limited to release notes, algorithms, flowcharts, diagrams, notes, notebooks, and manuals.

2. All Source Code for all software used in or by, and/or incorporated in the Accused Functionalities of the Supplied Equipment, including all versions of such source code.

3. Documents sufficient to identify the version histories of all software and hardware used in or by the Supplied Equipment.

4. Documents sufficient to show the security features and tamper resistance of any hardware components in the Supplied Equipment responsible for storing, generating, or using cryptographic keys including but not limited to:

   a. Documents that constitute, refer to or relate to any software, firmware or hardware incorporated into any of the Supplied Equipment that satisfy the requirements of FIPS 140-2 Level 3 in any areas; and

   b. Documents that constitute, refer to or relate to tamper protection of physical perimeters of hardware components of the Supplied Equipment including physical integrity checks performed before and during playback of Content.

5. All software, firmware, or hardware incorporated into any of the Supplied Equipment, and all documents and things referring to or related to such software, firmware, or hardware, that are involved in performing the functions described in the DCI Specification, including but not limited to the following functions:

a. providing and implementing a user interface (for example, at an SMS, TMS, projection system, or other user interface) to control playback of Content;

b. sending and receiving communications between all DCI-compliant Equipment, including SMS, TMS, media servers, Media Blocks, SPBs, and projection systems, to initiate and control playback of Content;

c. receiving, importing, storing, or ingesting encrypted Content, such as, but not limited to, Digital Cinema Packages and encrypted Track Files, Composition Playlists, and Key Delivery Messages;

d. converting packaged, compressed and encrypted data into raw image, sound and subtitles for playback of Content, including, but not limited to, unpacking packaged content from storage and arranging Track Files into their respective appropriate modules, decompressing or decoding compressed Content, and decrypting encrypted Content;

e. synchronizing the playback of image, audio, and other time-dependent Content;

f. providing a secure environment to decrypt encrypted Content;

g. forensically marking decrypted Content;

h. authenticating remote Secure Processing Blocks and Screen Management Systems (SMS) by establishing Transport Layer Security (TLS) sessions, and maintaining certificate lists collected;

i. validating Composition Playlists and logging results;

j. verifying that Content keys required for playback of Content are available and valid for scheduled exhibitions;

k. verifying that equipment used for the playback of Content is on a Trusted Device List received as part of a Key Delivery Message;

l. validating and decrypting Key Delivery messages;

m. collecting and storing log records and log information from remote Secure Processing Blocks and generating, digitally signing, storing, filtering, validating, auditing, and transmitting log reports and log records;

n. verifying that the conditions for playback specified in a KDM are satisfied;

o. issuing Content keys to a Media Decryptor;

p. generating keys for link encryption/decryption and encrypting/decrypting Content with such generated keys;

q. monitoring and logging integrity status and security-related events associated with a Media Block and remote Secure Processing Blocks and responsive actions in relation to such integrity status and security-related events;

r. enabling playback for a start time within the authorized time window for playback specified in a KDM;

s. processing Track File integrity pack metadata during playback, and logging any integrity pack deviations (including HMAC) detected;

t. determining that a specific Media Decryptor matches the key type IDs designated in a KDM;

u. receiving, authenticating, and executing software/firmware update files for all DCI-compliant Equipment, including SMS, TMS, storage systems and servers, Media Blocks, SPBs, and projection systems, and the storage, protection, and use of any associated cryptographic keys, root keys, and/or digital certificates;

v. authenticating digital certificates, including but not limited to digital certificates used in CPLs, packing lists, and KDMs;

w. providing physical security and tamper resistance around hardware modules, including secure silicon components and hardware module perimeter protection;

x. verifying that software and hardware comply with the DCI Specification and issuing certificates attesting to such compliance; and

y. verifying the integrity and/or authenticity of software, firmware, certificates, keys, or other data as part of a secure boot sequence or integrity status checking mechanism.

6. All documents that constitute, refer, or relate to the design, specification, architecture, operation, installation, usage and/or modification of each Supplied Equipment as it relates to the Accused Functionalities of the Supplied Equipment, including but not limited to design, function, engineering, architecture, system, user programming, and optimization guides/specifications, user manuals, datasheets, service manuals, instruction manuals, release notes, conceptual design documents, document repositories (*e.g.*, internal "wiki" pages, SharePoint, bug/deficiency tracking system contents), software and/or Source Code, firmware/microcode, flow charts, block diagrams, API documents, and/or circuitry maps.

7. All communications between you and any Defendant regarding the design, specification, architecture, operation, functionality, installation, testing, sales, leasing, usage and/or modification of the hardware, software and/or firmware of each Supplied Equipment as it relates to the Accused Functionalities of the Supplied Equipment.

8. All documents that constitute, refer, or relate to digital certificates; cryptographic keys, signatures, licenses, or hashes; or unique hardware or software entity identifiers; used in or by, or incorporated in the Supplied Equipment, including but not limited to:

a. Your generation and/or issuance of digital certificates, cryptographic keys, signatures, hashes, or other unique identifiers to the Supplied Equipment before or after a third party issues certifications of compliance of the Supplied Equipment with any part of the DCI Specification;

b. How digital certificates, cryptographic keys, or unique identifiers are assigned to any components of the Supplied Equipment; and

c. Use of certificates to implement any Accused Functionalities of the Supplied Equipment, including but not limited to use and authentication of certificates, cryptographic signatures or hashes, or unique identifiers in DCPs, CPLs, KDMs, packing lists, and Extra-Theater Messages (ETMs) to indicate DCI compliance.

9. Documents sufficient to show all aspects of your technical and commercial relationships with any Defendant or third party intermediary between you and any Defendant with respect to any of the Supplied Equipment.

10. Your communications, or any of your agents' communications, that pertain to Intertrust, any of the Cases, or any of the Asserted Patents.

11. For each Supplied Equipment, documents sufficient to show the technical requirements requested or imposed by any Defendant for any of the Accused Functionalities of the Supplied Equipment.

12. All documents referring to, relating to, or constituting testing or evaluation relating to the Supplied Equipment, including but not limited to alpha and beta testing, quality assurance

testing, compliance testing, and consumer testing and all results, outcomes, or conclusions of such testing, including all third-party testing relating to DCI certification or compliance, including the information mentioned in Chapters 9 and 10 of the Compliance Test Plan[13] supplied to any independent testing lab in connection with DCI certification.

13. For each Supplied Equipment, documents sufficient to show:

a. the full name of the Supplied Equipment;

b. the product indicia used by each Defendant and/or you to identify the Supplied Equipment;

c. the number of units you provided to each Defendant or to any third party intermediary between you and each Defendant of the Supplied Equipment;

d. the number of software/firmware field updates that you distributed for the Supplied Equipment;

e. the price each Defendant or said third party intermediary paid per unit of the Supplied Equipment;

f. pricing policies, guidelines and documents related to establishing prices for the Supplied Equipment;

g. overhead, indirect costs, or other allocated costs relevant to the sale, lease, or license of Supplied Equipment;

h. all revenues, payments, and profits you received from each Defendant or said third party intermediary in connection with the license, sale, or use of the Supplied Equipment; and

[13] See Attachment O.

i. any services, installation, maintenance, subscription, repairs or consulting provided by you in connection with the Supplied Equipment to each Defendant or said third party intermediary.

14. Internal and external financial statements to the extent they include notes or commentary regarding the development, production, sale, or servicing of any Supplied Equipment.

15. Product line profit and loss statements and/or product line income statements for the product lines that include the Supplied Equipment.

16. Budgets, forecasts, strategic plans, financial plans, business plans or management reports related to the research, development, testing, financing, marketing, sale, lease, or license of Supplied Equipment.

17. Product information sheets, training materials, or marketing materials or brochures related to the Supplied Equipment.

18. Documents sufficient to show your provision of Supplied Equipment having one or more of the Accused Functionalities to any Defendant, including but not limited to documents regarding negotiations, offers to contract, side letters or side agreements, bids, bid solicitations, responses to bid solicitations, requests for proposals, responses to requests for proposals, proposals, term sheets, purchase orders, loan documents, draft or final agreements, and related communications.

19. Documents sufficient to show your provision of engineering and/or manufacturing services to any Defendant relating to the Accused Functionalities of each Supplied Equipment, including but not limited to documents regarding negotiations, offers to contract, side letters or side agreements, bids, bid solicitations, responses to bid solicitations, requests for proposals,

responses to requests for proposals, proposals, purchase orders, draft or final agreements, and related communications.

20. Customer surveys that refer or relate to the Supplied Equipment.

21. Market studies, reports, forecasts or analyses, including reports on competitors and competing products, market segments, and customer demand for the Supplied Equipment.

22. For each Supplied Equipment:

a. any license agreements involving technology employed by the Supplied Equipment;

b. internal or third-party valuations or appraisals of technology employed by the Supplied Equipment;

c. royalty reports or documents that identify the amounts paid or received under license agreements for technology incorporated in the Supplied Equipment and documents sufficient to show the basis for calculating payments; and

d. documents and correspondence related to negotiations for the sale, license or transfer of interests or rights in technology employed by the Supplied Equipment, whether or not a transaction was ultimately consummated.

23. All documents regarding the benefits or advantages associated with each Supplied Equipment having the Accused Functionalities, including but not limited to all documents identifying cost savings, cost/benefit analyses, increased revenue/profit generation, improved picture quality or performance, customer reviews, and/or marketing research regarding each Supplied Equipment and prior products that the Supplied Equipment replaced.

24. All documents referring to, relating to, or constituting any analysis or opinion as to the infringement of the Asserted Patents by the Supplied Equipment.

25. All documents referring or related to laser projection or LED display technology provided or to be provided to Defendants or any intermediaries between you and Defendants to exhibit Content, including:

a. Product names, product numbers, model names, model numbers, internal codenames, internal product names, internal product numbers, and unique identifiers corresponding to equipment using such laser projection or LED display technology;

b. Price paid or to be paid for each equipment using such laser projection or LED display technology by Defendants or said third party intermediaries;

c. Benefits of equipment using such laser projection or LED display technology.

26. Documents sufficient to show the format, fields, and contents of log reports, KDMs, CPLs, and DCPs that are generated, processed, and/or received by the Supplied Equipment, including samples of the same.

27. Documents sufficient to show how software and firmware of the Supplied Equipment is updated, such as but not limited to, delivery, encryption, decryption, authentication, signing, installation, and formatting of such software/firmware updates for the Supplied Equipment, including samples of software/firmware updates and any associated software key distribution message files (SWKDM).

28. All documents referring to, relating to, or constituting all of the processing environments in the Supplied Equipment, including information about the architecture, design, and structure of the processing environments, such as but not limited to how access privileges and resources (*e.g.*, access to memory, secure silicon, cryptographic keys, etc.) are managed for the processing environments; documents showing the differences between the various processing

environments and how applications are executed separately from one another in these different processing environments to allow different applications to have different levels of access privileges and access to resources.