IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CARDWARE INC., Plaintiff v. SAMSUNG ELECTRONICS CO., LTD.; SAMSUNG ELECTRONICS AMERICA, INC., Defendants.	§ § § § § § § § § § § §	Civil Action No. 2:22-cv-00141-JRG-RSP JURY TRIAL DEMANDED

DEFENDANTS' NOTICE OF SUBPOENA TO APPLE INC.

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that pursuant to Rule 45 of the Federal Rules of Civil Procedure, Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Defendants"), have caused or will cause the attached subpoena for the production of documents and things to be served on Apple Inc. ("Apple"). The documents to be produced are specified in Attachment A to the subpoena.

PLEASE TAKE FURTHER NOTICE that pursuant to Rules 30 and 45 of the Federal Rules of Civil Procedure, Defendants, by and through their attorneys, will take the oral deposition of Apple. The deposition will be taken before a duly qualified notary public or other officer authorized to administer oaths, and will be recorded by stenographic and videographic means, as well as any other means permitted under the Federal Rules of Civil Procedure. Apple is instructed to appear at the time and location specified in the subpoena ad testificandum, or at another mutually agreeable time and location.

DATED: December 9, 2022

By: */s/ Robert Laurenzi*

Allan M. Soobert
allansoobert@paulhastings.com
Kecia Reynolds (*pro hac vice*)
keciareynolds@paulhastings.com
David Valente (*pro hac vice*)
davidvalente@paulhastings.com
PAUL HASTINGS LLP
2050 M Street NW
Washington, D.C. 20036
Telephone: 202-551-1700
Facsimile: 202-551-1705

Robert Laurenzi
robertlaurenzi@paulhastings.com
PAUL HASTINGS LLP
200 Park Avenue
New York, NY 10166
Telephone: (212) 318-6000
Facsimile: (212) 319-4090

Melissa R. Smith (TX Bar No. 24001351)
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 S. Washington Ave.
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Attorneys for Defendants Samsung Electronics Co., Ltd. and Samsung Electronics America, Inc.

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document has been served via email on all counsel of record on this 9th day of December, 2022.

/s/ Robert Laurenzi
Robert Laurenzi

CARDWARE EXHIBIT 2011
APPLE v. CARDWARE IPR2025-01150
Page 2 of 53

UNITED STATES DISTRICT COURT

for the

Eastern District of Texas

CardWare Inc. *Plaintiff* v. Samsung Electronics Co., Ltd., et al. *Defendant*	))))))	Civil Action No. 2:22-cv-00141-JRG-RSP

SUBPOENA TO TESTIFY AT A DEPOSITION IN A CIVIL ACTION

To: Apple Inc. c/o CT Corporation System
330 N. Brand Boulevard, Suite 700, Glendale, CA 91203
(Name of person to whom this subpoena is directed)

☑ *Testimony:* **YOU ARE COMMANDED** to appear at the time, date, and place set forth below to testify at a deposition to be taken in this civil action. If you are an organization, you must designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on your behalf about the following matters, or those set forth in an attachment:
See Attachment A

Place: Paul Hastings LLP 1117 S. California Ave Palo Alto, CA 94304	Date and Time: 01/23/2023 9:00 am

or a mutually agreeable location to be determined
The deposition will be recorded by this method: videograpically and stenographically

☑ *Production:* You, or your representatives, must also bring with you to the deposition the following documents, electronically stored information, or objects, and must permit inspection, copying, testing, or sampling of the material:
See Attachment A.
All documents and things must be produced and/or made available for inspection by January 9, 2023

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: 12/09/2022

CLERK OF COURT

OR

Signature of Clerk or Deputy Clerk	/s/ Robert Laurenzi *Attorney's signature*

The name, address, e-mail address, and telephone number of the attorney representing *(name of party)* Defendants Samsung Electronics Co., Ltd., et al., who issues or requests this subpoena, are:
Robert Laurenzi, Paul Hastings LLP, 200 Park Avenue NY, NY 10166, robertlaurenzi@paulhastings.com, 212-318-6000

Notice to the person who issues or requests this subpoena

If this subpoena commands the production of documents, electronically stored information, or tangible things 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. 2:22-cv-00141-JRG-RSP

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 individual 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

DEFINITIONS

1. The terms "You," "Your," or "Apple" mean and refer to Apple Inc. including all predecessors, successors, subsidiaries, divisions, and/or affiliates thereof, past or present, and all past or present officers, directors, agents, employees, consultants, accountants, attorneys, representatives, and any other person or entity acting on behalf of any of the foregoing.

2. The terms "CardWare" or "Plaintiff" mean and include CardWare Inc., a California corporation with its principal place of business located at 5201 Great America Parkway, Santa Clara, CA 95054, including all predecessors, successors, subsidiaries, divisions, parents and/or affiliates thereof, past or present, and all past or present officers, directors, agents, employees, consultants, accountants, attorneys, representatives, and any other person or entity acting on behalf of any of the foregoing.

3. The terms "Samsung" or "Defendant" mean and include Samsung Electronics Co. Ltd., and/or Samsung Electronics America, Inc., including all predecessors, successors, subsidiaries, divisions, parents and/or affiliates thereof, past or present, and all past or present officers, directors, agents, employees, consultants, accountants, attorneys, representatives, and any other person or entity acting on behalf of any of the foregoing.

4. The term "Asserted Patents" means U.S. Patent Nos. 10,339,520 ("the '520 patent"), 10,628,820 ("the '820 patent"), 10,810,579 ("the '579 patent"), 11,176,538 ("the '538 patent"), and 11,328,286 ("the '286 patent"), collectively and individually.

5. "Related Patents" means any or all: (a) United States patent applications which claim priority to the Asserted Patents, (b) United States patent applications or United States provisional applications from which priority is claimed by the Asserted Patents, (c) United States

patent applications which claim priority to a patent application or provisional application identified in (a) and/or (b), (d) any reissue or reexamination of any of the aforementioned patents or patent applications, and/or (e) foreign counterpart patents or patent applications (including any unpublished applications) to any of (a), (b), (c) or (d). The term "United States patent applications" as used in (a), (b), (c), and (d) includes, without limitation, all issued, abandoned, and pending patent applications.

6. "Document" and "documents" are synonymous in meaning and equal in scope to the usage of the terms as defined by Federal Rule of Civil Procedure 34, and include all things within the meaning and scope of that term as used in the Federal Rules of Civil Procedure, and the Federal Rules of Evidence, and includes without limitation, any document, writing, communication, or record, including without limitation the original of, copies of, and versions stored on electronic or digital media of correspondence, letters, memoranda, drafts, notes, notebooks, laboratory reports, translations, data compilations including all information stored on electronic media, electronic mail, telecopy or facsimile messages, reports, publications, computer printouts, charts, graphs, photographs, summaries or records of telephone conversations, summaries or records of personal conversations or interviews, minutes or records of meetings or conferences, or any other data compilation from which information can be obtained or translated, if necessary, through detection devices into reasonably usable form.

7. "Thing" and "things" have the broadest meaning allowable under Federal Rule of Civil Procedure 34. This meaning encompasses any tangible object of any kind and nature other than a document, including without limitation prototypes, models, and physical specimens thereof.

8. "Communication" or "communications" means any oral, written, or other contact

between or among two or more persons or entities by which any information or knowledge of any nature is transmitted or conveyed or attempted to be transmitted or conveyed, including correspondence, letters, memoranda, telegrams, telefaxes, telecopies, telexes, emails, text messages, face-to-face meetings, telephone conversations, voicemails, answering machine messages, and telephonic notes.

9. "Related," "relating," or "concerning" means comprising, pertaining, describing, referring, evidencing, discussing, showing, constituting, embodying, containing, reflecting, identifying, or in any way logically or factually connected with the matter discussed.

10. "Entity" or "entities" means any legal person, corporation, company, partnership, sole proprietorship, firm, board, joint venture, association, organization, trust, governmental body, agency, authority, commission, or any other juristic person, business unit, or collective organization, and any legal, governmental, organizational, or political subdivision thereof.

11. "Person" or "persons" means any natural person, individual, group, or entity. The acts of a person shall include the acts of the person's directors, officers, owners, members, employees, agents, attorneys, and all other representatives acting on the person's behalf.

12. "And," "or," and "and/or" shall be construed conjunctively or disjunctively, whichever maximizes the scope of each request in which they are used.

13. "Any" means "all" and/or "each" and vice versa, as necessary to bring within the scope of the request all information that might otherwise be construed to be outside the scope.

14. "Each" and "every" shall be construed to mean "each and every."

INSTRUCTIONS

The following instructions apply to each specific request unless otherwise explicitly stated.

1. You are to search all Documents within Your possession, custody, or control, wherever located, including any Documents placed in storage facilities or in the possession of any employee, agent, representative, attorney, investigator, or other person acting or purporting to act on Your behalf (whether located at his/her residence or place of business), in order to fully respond to the requests herein.

2. You are to produce Documents from any single file in the same order as they were found in such file, including any labels, files, folders and/or containers in which such Documents are located in or associated with. If copies are produced in lieu of the originals, such copies should be legible and bound, stapled, or segregated in the same manner as the original.

3. If You do not produce each Document or thing requested herein as they are kept in the usual course of business, You must organize and label the Documents or things produced to correspond with the particular document request to which the Document or thing is responsive.

4. You are to produce all Documents which are responsive in whole or in part to any of the requests herein in full, without abridgement, abbreviation, or expurgation of any sort. If any such Documents cannot be produced in full, produce the document to the extent possible.

5. You are required to produce not only the original or an exact copy of the original of all Documents or things responsive to any of the requests herein, but also all copies of such Documents or things which bear any notes or markings not found on the originals and all preliminary, intermediate, final, and revised drafts or embodiments of such Documents or things.

You are also required to produce all versions of the foregoing Documents stored by a computer internally, on disk, on CD-ROM, or on tape.

6. You are to produce any purportedly privileged Document containing non-privileged matter, with the purportedly privileged portion excised or redacted.

7. If any of the Documents requested herein are no longer in Your possession, custody, or control, You are requested to identify each such requested Document by date, type of Document, person(s) from whom sent, person(s) to whom sent, and person(s) receiving copies, and to provide a summary of its pertinent contents.

8. If any Document responsive to these requests has been destroyed, describe the content of such Document, the location of any copies of such Document, the date of such destruction, and the name of the person who ordered or authorized such destruction.

9. Electronic and computerized materials must be produced in an intelligible format or together with a description of the system from which it was derived sufficient to permit tendering of the material intelligible.

10. If any of the Documents or things are considered "confidential" such Documents or things should be produced subject to the terms and provisions of the Protective Order (Ex. 6).

11. If production of any Document listed and described in Attachment A hereto is withheld on the basis of a claim of privilege, each withheld Document shall be separately identified in a privileged document list. The privileged document list must identify each Document separately, specifying for each Document at least: (1) the date; (2) author(s)/sender(s); (3) recipient(s), including copy recipients; and (4) general subject matter of the document. The sender(s) and recipients(s) shall be identified by position and entity (corporation or firm, etc.) with which they are employed or associated. If the sender or the recipient is an attorney or a

foreign patent agent, he or she shall be so identified. The type of privilege claimed must also be stated, together with a certification that all elements of the claimed privilege have been met and have not been waived with respect to each Document.

REQUESTS FOR PRODUCTION

REQUEST FOR PRODUCTION NO. 1:

Documents, communications, and things describing Apple's conception and reduction to practice of Apple Pay's use of tokenization (replacing the Primary Account Number/credit card number with a token or substitute number), a dynamic limited-use cryptogram, and NFC (or other wireless communication technology) to accomplish a mobile transaction prior to the commercial launch of Apple Pay in October 2014. *See* Exs. 1–3.

REQUEST FOR PRODUCTION NO. 2:

Documents, communications, and things describing Apple's discussions with Visa, MasterCard and AmericanExpress or any third party merchant, bank, payment provider, standards organization, or clearance house, regarding mobile payments using tokenization, dynamic limited-use cryptograms, and NFC (or other wireless communication technology), prior to the 2014 commercial launch of Apple Pay. This request includes, but is not limited to, discussions that occurred in January 2013 with Visa, MasterCard and AmericanExpress as described in Exhibit 4 ("The financial industry began working on the Apple Pay project in January 2013, when Apple had the first concrete conversations with the big credit card networks, Visa, MasterCard and AmericanExpress, after years of more vague conversations about the best way for Apple to get involved.")

REQUEST FOR PRODUCTION NO. 3:

Documents, communications, and things sufficient to describe Apple's discussions and interactions with EMVCo regarding mobile payments using tokenization, dynamic limited-use cryptograms, and NFC (or other wireless communication technology) prior to the commercial launch of Apple Pay in 2014. This request includes, but is not limited to, documents,

communications, and things relating to the *EMV® Payment Tokenisation Specification - Technical Framework v1.0* referred to in Ex. 5, and all predecessor documents and drafts of the same.

REQUEST FOR PRODUCTION NO. 4:

All Documents, communications, and things concerning the Asserted Patents and Related Patents.

REQUEST FOR PRODUCTION NO. 5:

All Documents, communications, and things concerning CardWare, Virtual Electric, Inc. and David Wyatt.

DEPOSITION TOPICS

TOPIC NO. 1:

Apple's conception and reduction to practice of Apple Pay's use of tokenization (replacing the Primary Account Number/credit card number with a token or substitute number), a dynamic limited-use cryptogram, and NFC (or other wireless communication technology) to accomplish a mobile transaction prior to the commercial launch of Apple Pay in October 2014.

TOPIC NO. 2:

Apple's discussions with Visa, MasterCard and AmericanExpress or any third party standards committee, merchant, bank, payment provider or clearance house, regarding mobile payments using tokenization, dynamic limited-use cryptograms, and NFC (or other wireless communication technology), prior to the 2014 commercial launch of Apple Pay.

TOPIC NO. 3:

The accuracy and authenticity of Exhibits 1 through 3.

TOPIC NO. 4:

Apple's communications with CardWare, Virtual Electric, Inc. and David Wyatt, or relating in any way to the Asserted Patents.

Exhibit 1

Unable to decrypt apple pay token

Enabling an apple pay support in web app and processing the payment via Cybersource payment gateway.

Apple Payment token received as part of payment has been sent to cybersource for payment processing.

8.9k

CyberSource is saying token is not valid and unable to decrypt. Cybersource is expecting token length to arround 3000 to 5000.

Token Reeived from apple is around 500.

Here is the token , its length is 425 . What am i missing here. What is the minimum length of Apple Pay token, Can you share any reference to payment token length.

"8d5eLdUWgmd8RutsBaxdBsJhnpxUe2lYC/B7cgtgwASHa5+kz7hmNLhqH3+eKGlEW3hwOlTGPoY64Pe/vWhd3EjKPwltYqfz9wyZqQjWV5wYUHjFEUtUYeHmnf0O1KVpP656IncK/jNT+vgm2sTiUxBLWTyCZmnBQsiDjjaD0eEQLB7aNQ2nVdEpEDjXcZhl0JjwXS1hQ3KH2Hcvk+1UduiBx1jXYlBSPuCSEP8Q3slTdEbFQf9LF2rerN3WavaqeBClf5PqtluuUJkRdwoR80SQ9vEk3KpKmaFvOZaaJXCrkurhxklje5ZJUyrMrKwSU7HvswDnHvPqT1Wyk3SD/EDa5/61/hZfeMtDtLvAsuN8nq2h3gER2lya3BxZCV0qWeuzqy4IAw0r7u19Bq2+8OTwY6pPkx6cQDyS/4jO"

Thanks

Wallet

Reply

Posted 5 years ago by NotANameTest

Add a Comment

Replies

It depends....quoting off the 'net:

What is an Apple Pay PKPaymentToken?
The PKPaymentToken is an encrypted data package created by the Apple Pay server using your public key. This package contains several components including the network token and a cryptogram.

What is the cryptogram?
The cryptogram returned by Apple Pay is a component of the PKPaymentToken that is unique to the transaction and acts as a security key. It is 40 characters in length and created using the merchant's public key supplied to Apple during the merchant registration process.

What is a network token?
A network token is a surrogate value for a PAN that is between 13 and 19 digits (typically format preserving) and is MOD-10 compliant (passes Luhn check). All network tokens will use BIN ranges designated for tokens and never overlap or conflict with a real PAN.
>CyberSource is saying token is not valid and unable to decrypt

Confirm your process:
- h ttp://apps.cybersource.com/library/documentation/dev_guides/apple_payments/SO_API/Apple_Pay_SO_API.pdf
- *https://developer.apple.com/library/content/documentation/PassKit/Reference/PaymentTokenJSON/PaymentTokenJSON.html#//apple_ref/doc/uid/TP40014929-CH8-SW1*

Posted 5 years ago by KMT

Add a Comment

Hi, here we are having same issue. We uploaded CSR to "Apple Pay Payment Processing Certificate" section but when we submit request to cybersource we get Unable to decrypt encrypted_payment_data.

Do you have found the solution?

Posted 2 years ago by d.colaianni

Add a Comment

Any Solution...????

Posted 1 year ago by sandy_cool

Add a Comment

You need to take the entire paymentToken received from onpaymentauthorized, get the paymentData, then base64 encode

response will look like this

`Payment Token: { "paymentData": { "version": "EC_v1", "data":
"UwXPzQeEmi+IgZp9Tz6lEhLNmXmZrQ2FqdNYs671/sE/3rqOpcKrZOGPHu9JMGIHZZOFkbVPAQ919wmLfWLXKIvqxbpAz
Joc1F9NjtZmWpiqJELCzPTbdi+OmQrggnBAw8fd7FwVY19bNDoqtN5g4lSeV2Gs1nTzRjvWb7W17+J5dlq/cOK0RCD/O8mjw
YQ5axrZc6WrWXoAhdwsNf9dLqdTeCPEW2rkccikmr2670DFYhSMyF+JrG4aHmDBY7v8EHgvkdd2fjPB92Qh4j4UEa0i6/oO
Z4VC7u3svNYEwGEBXbjMkpQr4UPfkuxGaxTvAJBg3ra+x6WGIEAwzHKkoenIf9NkBbFJmHdJ5ZD1GbzL7b8cBilnL/si3/sSm
GMgI7m68noFIKetDZwlN9P2+5RnofcECN5FM/aR5vpzrA==", "signature":
"MIAGCSqGSIb3DQEHAqCAMIACAQExDzANBglghkgBZQMEAgEFADCABgkqhkiG9w0BBwEAAKCAMIID5DCCA4ugAwIBAg
IIWdihvKr0480wCgYIKoZIzj0EAwIwejEuMCwGA1UEAwwIQXBwbGUgQXBwbGljYXRpb24gSW50ZWdyYXRpb24gQ0EgLSB
HMzEmMCQGA1UECwwdQXBwbGUgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxEzARBgNVBAoMCkFwcGxlIEluYy4xCzAJB
gNVBAYTAlVTMB4XDTIxMDQyMDE5MzcwMFoXDTI2MDQxOTE5MzY1OVowYjEoMCYGA1UEAwwfZWNjLXNtcC1icm9rZXIt
c2lnbl9VQzQtU0FOREJPWDEUMBIGA1UECwwLaU9TIFN5c3RlbXMxEzARBgNVBAoMCkFwcGxlIEluYy4xCzAJBgNVBAYTAl
VTMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEgjD9q8Oc914gLFDZm0US5jfiqQHdbLPgsc1LUmeY+M9OvegaJajCHkwz
3c6OKpbC9q+hkwNFxOh6RCbOlRsSlaOCAhEwggINMAwGA1UdEwEB/wQCMAAwHwYDVR0jBBgwFoAUI/JJxE+T5O8n5sT
2KGw/orv9LkswRQYIKwYBBQUHAQEEOTA3MDUGCCsGAQUFBzABhilodHRwOi8vb2NzcC5hcHBsZS5jb20vb2NzcDA0LW
FwcGxlYWljYTMwMjCCAR0GA1UdIASCARQwggEQMIIBDAYJKoZIhvdjZAUBMIH+MIHDBggrBgEFBQcCAjCBtgyBs1JlbGlhb
mNlIG9uIHRoaXMgY2VydGlmaWNhdGUgYnkgYW55IHBhcnR5IGFzc3VtZXMgYWNjZXB0YW5jZSBvZiB0aGUgdGhlbiBhcH
BsaWNhYmxlIHN0YW5kYXJkIHRlcm1zIGFuZCBjb25kaXRpb25zIG9mIHVzZSwgY2VydGlmaWNhdGUgcG9saWN5IGFuZCBj
ZXJ0aWZpY2F0aW9uIHByYWN0aWNlIHN0YXRlbWVudHMuMDYGCCsGAQUFBwIBFipodHRwOi8vd3d3LmFwcGxlLmNvbS
9jZXJ0aWZpY2F0ZWF1dGhvcml0eS8wNAYDVR0fBC0wKzApoCegJYYjaHR0cDovL2NybC5hcHBsZS5jb20vYXBwbGVha
WNhMy5jcmwwHQYDVR0OBBYEFAIkMAua7u1GMZekplopnkJxghxFMA4GA1UdDwEB/wQEAwIHgDAPBgkqhkiG92NkBh0E
AgUAMAoGCCqGSM49BAMCA0cAMEQCIHShsyTbQklDDdMnTFB0xICNmh9IDjqFxcE2JWYyX7yjAiBpNpBTq/ULWlL59gBN
xYqtbFCn1ghoN5DgpzrQHkrZgTCCAu4wggJ1oAMCAQICCEltL786mNqXMAoGCCqGSM49BAMCMGcxGzAZBgNVBAMME
kFwcGxlIFJvb3QgQ0EgLSBHMzEmMCQGA1UECwwdQXBwbGUgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkxEzARBgNVBAo
MCkFwcGxlIEluYy4xCzAJBgNVBAYTAlVTMB4XDTE0MDUwNjIzNDYzMFoXDT[illegible]MCAwMUEAww

CARDWARE EXHIBIT 2011
APPLE v. CARDWARE IPR2025-01150
Page 17 of 53

lQXBwbGUgQXBwbGljYXRpb24gSW50ZWdyYXRpb24gQ0EgLSBHMzEmMCQGA1UECwwdQXBwbGUgQ2VydGlmaWNhd
GlvbiBBdXRob3JpdHkxEzARBgNVBAoMCkFwcGxlIEluYy4xCzAJBgNVBAYTAlVTMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQ
gAE8BcRhBnXZIXVGl4lgQd26ICi7957rk3gjfxLk+EzVtVmWzWuItCXdg0iTnu6CP12F86Iy3a7ZnC+yOgphP9URaOB9zCB9D
BGBggrBgEFBQcBAQQ6MDgwNgYIKwYBBQUHMAGGKmh0dHA6Ly9vY3NwLmFwcGxlLmNvbS9vY3NwMDQtYXBwbGVyb
290Y2FnMzAdBgNVHQ4EFgQUl/JJxE+T5O8n5sT2KGw/orv9LkswDwYDVR0TAQH/BAUwAwEB/zAfBgNVHSMEGDAWgBS7
sN6hWDOImqSKmd6+veuv2sskqzA3BgNVHR8EMDAuMCygKqAohiZodHRwOi8vY3JsLmFwcGxlLmNvbS9hcHBsZXJvb3R
jYWczLmNybDAOBgNVHQ8BAf8EBAMCAQYwEAYKKoZIhvdjZAYCDgQCBQAwCgYIKoZIzj0EAwIDZwAwZAIwOs9yg1EWmb
GG+zXDVspiv/QX7dkPdU2ijr7xnIFeQreJ+Jj3m1mfmNVBDY+d6cL+AjAyLdVEIbCjBXdsXfM4O5Bn/Rd8LCFtlk/GcmmCEm9U
+Hp9G5nLmwmJIWEGmQ8Jkh0AADGCAYwwggGIAgEBMIGGMHoxLjAsBgNVBAMMJUFwcGxlIEFwcGxpY2F0aW9uIEludG
VncmF0aW9uIENBIC0gRzMxJjAkBgNVBAsMHUFwcGxlIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MRMwEQYDVQQKDApBc
HBsZSBJbmMuMQswCQYDVQQGEwJVUwIIWdihvKr0480wDQYJYIZIAWUDBAIBBQCggZUwGAYJKoZIhvcNAQkDMQsGCS
qGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwNjE3MTI1MDM1WjAqBgkqhkiG9w0BCTQxHTAbMA0GCWCGSAFlAwQC
AQUAoQoGCCqGSM49BAMCMC8GCSqGSIb3DQEJBDEiBCBTS7/cJTkqoPngqDvEXQixx62F3leq4oEk+vRLItaWeTAKBggq
hkjOPQQDAgRHMEUCIA+MBrjOk3i/zTJ6xiHOOKUtN6dfYdqgstciP/bP0Ig9AiEA+vXLBd0Xlhbe03b3AJbHW7XotUu3gt3clM
psv6e//0EAAAAAAAA=", "header": { "ephemeralPublicKey":
"MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEL7u/GO5+iFC5hK0516IgX6DKmPB0xTi3oQ1nWCdTc5DXQuAP4XMep40jG
Rb7UCoaEXgPx5vvRuxshadS7PP4+w==", "publicKeyHash": "ilecVF58bpB8qio67Y0Okg5Hl6eirw2Y1v1KUCsdVgQ=",
"transactionId": "92fc14bc748dd361f563d0a0a24fddb5d96715ef9a491b546274ed5e05463c2b" } }, "paymentMethod":
{ "displayName": "Visa 0492", "network": "Visa", "type": "debit" }, "transactionIdentifier":
"92FC14BC748DD361F563D0A0A24FDDB5D96715EF9A491B546274ED5E05463C2B" }

JS send to backend as applepay_data '&applepay_data=' + encodeURIComponent(JSON.stringify(token.paymentData));

Java example to base64 encode String applePayToken = reqParms.getString("applepay_data",null); byte[] encodedBytes = Base64.encodeBase64(applePayToken.getBytes(StandardCharsets.UTF_8)); applePayToken = new String(encodedBytes,StandardCharsets.UTF_8);

That is what you need to send to Cybersource, if you are just sending part of token.paymentData it won't work

Posted 1 year ago by jbcle

Add a Comment

This site contains user submitted content, comments and opinions and is for informational purposes only. Apple disclaims any and all liability for the acts, omissions and conduct of any third parties in connection with or related to your use of the site. All postings and use of the content on this site are subject to the Apple Developer Forums Participation Agreement.

CARDWARE EXHIBIT 2011
APPLE v. CARDWARE IPR2025-01150
Page 18 of 53

Safari & Web

To view the latest developer news, visit News and Updates .

Copyright © 2022 Apple Inc. All rights reserved. Terms of Use | Privacy Policy | License Agreements

CARDWARE EXHIBIT 2011
APPLE v. CARDWARE IPR2025-01150
Page 19 of 53

Exhibit 2

PassKit (Apple Pay and Wallet)

- PKPaymentRequestShippingContactUpdate
- PKPaymentRequestShippingMethodUpdate
- PKPaymentRequestCouponCodeUpdate
- PKPaymentRequestUpdate
- QR Transaction Information
- PKPaymentInformationEventExtension
- PKPaymentInformationRequestHandling
- Entitlements
- Merchant IDs Entitlement
- Payment Token Format
- Payment Token Format Reference
  - Symmetric Keys
    - Restoring the Symmetric Key
- Errors
- PKPaymentError
- PKPaymentErrorKey
- Deprecated
- PKAddressField Deprecated
- Wallet Support
- Wallet

Article

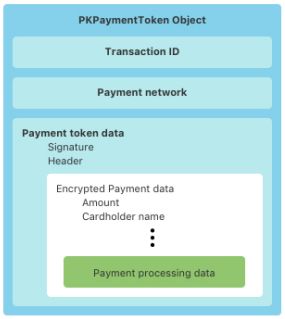
Payment Token Format Reference

Verify an Apple Pay payment token and validate a transaction.

Overview

Apple Pay is available on all iOS devices with a Secure Element — an industry-standard, certified chip designed to store payment information safely. In macOS, users must have an iPhone or Apple Watch that supports Apple Pay to authorize the payment, or have a Mac with Touch ID. The Secure Element creates a payment object when an app or website that uses Apple Pay sends a payment request.

The payment object has a nested structure that contains a payment token with encrypted payment data, as shown in the figure below.



The Secure Element encrypts the token's payment data using either elliptic curve cryptography (ECC) or RSA encryption. The Secure Element selects the encryption algorithm based on the merchant capabilities that the payment request indicates. Most regions use ECC encryption. Other regions use RSA encryption if ECC encryption is unavailable due to regulatory concerns.

Verify the Signature and Decrypt the Payment Data

The following steps describe the process of validating a transaction by verifying the signature, decrypting the payment data, and verifying additional transaction details. Refer to the reference tables to identify keys and values.

Step 1: Verify the signature as follows:

- Ensure that the certificates contain the correct custom OIDs: 1.2.840.113635.100.6.29 for the leaf certificate and 1.2.840.113635.100.6.2.14 for the intermediate CA. The value for these marker OIDs doesn't matter, only their presence.
- Ensure that the root CA is the Apple Root CA - G3. This certificate is available from www.apple.com/certificateauthority.
- Ensure that there's a valid X.509 chain of trust from the signature to the root CA. Specifically, ensure that the signature was created using the private key that corresponds to the leaf certificate, that the leaf certificate is signed by the intermediate CA, and that the intermediate CA is signed by the Apple Root CA - G3.
- Validate the token's signature. For ECC (EC_v1), ensure that the signature is a valid Ellyptical Curve Digital Signature Algorithm (ECDSA) signature (ecdsa-with-SHA256 1.2.840.10045.4.3.2) of the concatenated values of the `ephemeralPublicKey`, `data`, `transactionId`, and `applicationData` keys. For RSA (RSA_v1), ensure that the signature is a valid RSA signature (RSA-with-SHA256 1.2.840.113549.1.1.11) of the concatenated values of the `wrappedKey`, `data`, `transactionId`, and `applicationData` keys.
- Inspect the Cryptographic Message Syntax (CMS) signing time of the signature, as defined by section 11.3 of RFC 5652. If the time signature and the transaction time differ by more than 5 minutes, the token may be a replay attack.

> **Important**
> The signature is valid if all the signature verification steps above succeed. If the signature is invalid or any of the hash values don't match, ignore the transaction.

Step 2: Use the value of the `publicKeyHash` key to determine which merchant public key Apple used, and then retrieve the corresponding merchant public key certificate and private key.

Step 3: Restore the symmetric key. For instructions, see Restoring the Symmetric Key.

Step 4: Use the symmetric key to decrypt the value of the data key:

- For ECC (EC_v1), decrypt the data key using AES-256 (id-aes256-GCM 2.16.840.1.101.3.4.1.46) with an

initialization vector of 16 null bytes and no associated authentication data.

- For RSA (RSA_v1), decrypt the data key using AES–128 (id-aes128-GCM 2.16.840.1.101.3.4.1.6), with an initialization vector of 16 null bytes and no associated authentication data.

After you complete Step 4, the payment data in the `data` value of the payment token structure is decrypted. Use the decrypted payment data and information you have about the transaction to validate that transaction.

Step 5: Confirm that you haven't already credited this payment by verifying that no payment with the same `transactionId` shows as processed. For efficiency, consider only those payments with a transaction time that's within the 5-minute time window of the current `transactionId`, as explained in the last bullet point of Step 1.

Step 6: Verify the transaction details using information from the merchant about the Apple Pay payment request and other transaction information:

- Check that the `currencyCode` matches the currency code in the original Apple Pay payment request.
- Check that the `transactionAmount` is correct, as compared with the total charge of the transaction.
- Check that the `applicationData` field matches the hash of the data the original payment request used, and that the data is correct. For example, check that an order number in the data from the original payment request is the order number to which you, the payment processor, are applying this payment. For more information, see `applicationData` in `PKPaymentRequest`. For transactions that initiate in Apple Pay on the Web, see `applicationData` in `ApplePayPaymentRequest` and `applicationData` in `ApplePayRequest`.

Step 7: If the signature is valid, the hash values match, and your transaction validation passes, use the decrypted payment data to process the payment. Otherwise, ignore the transaction.

Payment Token Format Reference

The following tables describe the keys and values of the payment token structure.

Payment Token Structure

The `paymentData` property of `PKPaymentToken` (or the `paymentData` property of `ApplePayPaymentToken`, for Apple Pay on the Web) contains a UTF-8 serialization of a plaintext JSON dictionary with the following keys and values:

Key	Value	Description
`data`	payment data dictionary, Base64 encoded as a string	Encrypted payment data See Payment Data Keys below for the decrypted payment data keys and values.
`header`	header dictionary	Additional version-dependent information you use to decrypt and verify the payment See Header Keys and Values below.
`signature`	detached PKCS #7 signature, Base64 encoded as a string	Signature of the payment and header data The signature includes the signing certificate, its intermediate CA certificate, and information about the signing algorithm.
`version`	string	Version information about the payment token The token uses `EC_v1` for ECC-encrypted data and `RSA_v1` for RSA-encrypted data.

Header Keys and Values

The `header` contains the following keys and values:

`applicationData`	SHA–256 hash, hex encoded as a string	Optional. Hash of the `applicationData` property of the original `PKPaymentRequest` object for transactions that initiate in apps. For transactions that initiate in Apple Pay on the Web, the value is the hash of `applicationData` in `ApplePayPaymentRequest` or of `applicationData` in `ApplePayRequest`. This key is omitted if the value of that property is `nil`.
`ephemeralPublicKey`	X.509 encoded key bytes, Base64 encoded as a string	Ephemeral public key bytes EC_v1 only.
`wrappedKey`	A Base64-encoded string	The symmetric key wrapped using your RSA public key RSA_v1 only.
`publicKeyHash`	SHA–256 hash, Base64 encoded as a string	Hash of the X.509 encoded public key bytes of the merchant's certificate

`transaction Id`	A hexadecimal identifier, as a string	Transaction identifier, generated on the device

For more information about the application data and the original payment request, see `applicationData` and `PKPaymentRequest`. For transactions using Apple Pay on the Web, see `applicationData` and `ApplePayRequest`, and `applicationData` and `ApplePayPaymentRequest`.

Payment Data Keys

The decrypted payment data in the `data` value contains the following keys and values:

Key	Value	Description
`applicationPrimary AccountNumber`	string	Device-specific account number of the card that funds this transaction
`application ExpirationDate`	date as a string	Card expiration date in the format YYMMDD
`currencyCode`	string	ISO 4217 numeric currency code, as a string to preserve leading zeros
`transactionAmount`	number	Transaction amount
`cardholderName`	string	Optional. Cardholder name.
`deviceManufacturer Identifier`	string	Hex-encoded device manufacturer identifier
`paymentDataType`	string	Either `"3DSecure"` or `"EMV"`
`paymentData`	payment data dictionary	Detailed payment data; see Detailed Payment Data Keys (3D Secure) and Detailed Payment Data Keys (EMV) below
`authentication Responses`	list of Authentication Response entries	For a multitoken request, a list of submerchant responses that contain cryptograms. See Authentication Response below.
`merchantToken Identifier`	string	For a merchant token request, the provisioned merchant token identifier from the payment network
`merchantToken Metadata`	`MerchantToken Metadata`	For a merchant token request, this data contains card art and the token's last four digits and expiration date

Detailed Payment Data Keys (3D Secure)

If the `paymentDataType` value is `"3DSecure"` in the Payment Data Keys information, the payment data dictionary in `paymentData` contains the following keys and values:

Key	Value	Description
`onlinePayment Cryptogram`	A Base64-encoded string	Online payment cryptogram, as defined by 3D Secure
`eciIndicator`	string	Optional. ECI indicator, as defined by 3D Secure The card network may add an ECI indicator to the payment data that the payment token includes. If you receive an ECI indicator, you must pass it on to your payment processor; otherwise, the transaction fails.

Detailed Payment Data Keys (EMV)

If the `paymentDataType` value is `"EMV"` in the Payment Data Keys information, the payment data dictionary in `paymentData` contains the following keys and values:

Key	Value	Description
`emvData`	The Europay, Mastercard, and Visa (EMV) payment structure, as a Base64-encoded string	Output from the Secure Element
`encrypted PINData`	The encrypted PIN, as a hex-encoded string	The PIN is encrypted using the bank's key. RSA_v1 only.

Authentication Response

The dictionary for the `authenticationResponses` in the Payment Data Keys information contains the following keys and values:

CARDWARE EXHIBIT 2011
APPLE v. CARDWARE IPR2025-01150
Page 23 of 53

Key	Value	Description
`merchantIdentifier`	string	The submerchant identifier as provided by the coordinator merchant
`authenticationData`	string	Payment network-generated cryptogram for the submerchant
`transactionAmount`	string	The authorized amount for a given submerchant

Topics

Symmetric Keys

Restoring the Symmetric Key

Restore the symmetric key you use to verify payment data.

Filter

Platforms
iOS
iPadOS
macOS
tvOS
watchOS
Tools
Swift
SwiftUI
Swift Playgrounds
TestFlight
Xcode
Xcode Cloud
SF Symbols

Topics & Technologies
Accessibility
Accessories
App Extensions
App Store
Audio & Video
Augmented Reality
Business
Design
Distribution
Education
Fonts
Games
Health & Fitness
In-App Purchase
Localization
Maps & Location
Machine Learning
Security
Safari & Web

Resources
Documentation
Curriculum
Downloads
Forums
Videos
Support
Support Articles
Contact Us
Bug Reporting
System Status
Account
Apple Developer
App Store Connect
Certificates, IDs, & Profiles
Feedback Assistant

Programs
Apple Developer Program
Apple Developer Enterprise Program
App Store Small Business Program
MFi Program
News Partner Program
Video Partner Program
Security Bounty Program
Security Research Device Program
Events
Events Overview
App Accelerators
App Store Awards
Apple Design Awards
Apple Developer Academies
Entrepreneur Camp
Tech Talks
WWDC

To view the latest developer news, visit News and Updates.

Light Dark Auto

Copyright © 2022 Apple Inc. All rights reserved. Terms of Use | Privacy Policy | Agreements and Guidelines

Exhibit 3

Structure

ApplePayPaymentToken

An object that contains the user's payment credentials.

Safari Desktop 10.0+ Safari Mobile 10.0+

Declaration

```
dictionary ApplePayPaymentToken {
    required ApplePayPaymentMethod paymentMethod;
    DOMString transactionIdentifier;
    JSON paymentData;
};
```

Overview

You access the payment token of an authorized payment request using the `token` property of the `ApplePayPayment` object.

Topics

Payment Token Properties

`paymentMethod`

Information about the card used in the transaction.

`paymentData`

An object containing the encrypted payment data.

`transactionIdentifier`

A unique identifier for this payment.

CARDWARE EXHIBIT 2011
APPLE v. CARDWARE IPR2025-01150
Page 26 of 53

See Also

Payment Token

`token`

The encrypted information for an authorized payment.

`ApplePayPaymentMethod`

A dictionary that describes an Apple Pay payment method.

`ApplePayPaymentMethodType`

A string that represents the type of the payment method.

`ApplePayPaymentPass`

A provisioned payment card for Apple Pay payments.

Exhibit 4

The New York Times

Banks Did It Apple's Way in Payments by Mobile

By Nathaniel Popper September 11, 2014 9:11 pm

JPMorgan Chase's chief financial officer, Marianne Lake, took the stage at a financial conference on Tuesday under strict orders not to mention her company's involvement in Apple's new payment system.

But when Apple's chief executive, Timothy D. Cook, at a news conference in California at the same time, finally brought up Apple Pay, one of Ms. Lake's deputies in New York took a green apple out of her bag and put it on a table on the stage, signaling that Ms. Lake was free to discuss the service.

"So we are very excited about Apple Pay, and Chase customers will be able to participate in that," Ms. Lake said, noting the appearance of the apple with a nod of her head.

The elaborate measures that Ms. Lake took to keep Apple Pay under wraps until the chosen time underscore the degree of preparation — and investment — that went into a partnership that has the potential to transform one of the banking industry's most fundamental business lines.

For the banks and credit card networks, Apple Pay could threaten some revenue streams, as the technology giant looks to assume a more central role in the financial universe. But the eager participation of banks and card companies suggests both Apple's clout, and the recognition among financial institutions that they face broader

challenges from upstart technology ventures, many of which are not as eager or willing as Apple to work with the incumbent financial industry.

"There are schemes that don't respect and honor the payment networks," said James Anderson, the senior vice president for mobile product development at MasterCard. "We want to invest in programs that respect our role in the ecosystem."

The immediate cost of Apple Pay is expected to be assumed by the banks, which are offering Apple a lower rate than they normally accept from credit card transactions, according to people briefed on the agreements. The banks, which take the biggest chunk of credit card transaction fees, are hopeful that they will make up for the lower rates by processing new types of transactions that are currently being done with cash or other payment methods.

The big credit card networks will not have to pay any costs for working with Apple. But some analysts warned this week that Apple Pay could, in the long run, push down the rates that both credit card networks and banks can charge merchants. Credit card fees are largely used to cover the costs of fraud, which are expected to go down with Apple's fingerprint signature.

Even so, the partnership with Apple is much more attractive than an initiative being led by some of the biggest retailers, known as the Merchant Customer Exchange, that appears to be looking to replace the card networks altogether. That concern was brought to the fore on Thursday when two of the biggest supporters of the Merchant Customer Exchange, Walmart and Best Buy, announced that they would not accept Apple Pay.

And upstart projects like Bitcoin are looking to bypass the current financial system. Earlier this year, JPMorgan's chief executive, Jamie Dimon, told investors that the companies in Silicon Valley "all want to eat our lunch."

The financial industry has been under growing pressure to update the current, rather outdated, payment networks, which have been blamed for big breaches of customer data at retailers like Target and Home Depot.

The banks and card companies have dedicated enormous resources to finding their own technological improvements. The major cards and banks have all been working on a system that allows customers to make a payment without handing over any personal details, using a kind of digital token that can be used only once.

Apple Pay will be the first program to use the so-called tokenization system on a widespread basis, and financial firms are hopeful that this will point the way to a future payments system in which they are still central players.

“We can show the world this is where it’s all headed,” said Jim McCarthy, the global head of innovation and strategic partnerships at Visa. “This may be the inflection point where you can see a real improvement in what has been a clunky digital experience.”

The project has not persuaded everyone. Merchants will still have to install hardware that can read the wireless signal carrying the payment information from Apple’s devices. And past efforts at new mobile wallets, like Google Checkout, have not widely caught on.

The financial industry began working on the Apple Pay project in January 2013, when Apple had the first concrete conversations with the big credit card networks, Visa, MasterCard and American Express, after years of more vague conversations about the best way for Apple to get involved.

From the beginning, the project was top secret, with what one person involved called a “code name frenzy.” The card companies had code names for Apple and Apple for the card companies. At Visa, the code name was another consumer electronics company, chosen to avert attention from employees who were not involved. Visa soon had about a thousand people on the team.

In the summer of 2013, Apple approached each of the five major banks involved in the project, without revealing what other banks were involved.

JPMorgan, the largest card issuer in the country, set up a war room in a windowless conference room in San Francisco, where the most sensitive work was

done. Only about 100 of the 300 JPMorgan employees working on the project knew that it was a partnership with Apple.

The project remained a top secret until the final moments.

JPMorgan put a live stream of the Apple event on the large screens of the lobby of its headquarters in New York, without being able to explain the bank's involvement in the proceedings.

Even the people involved most closely in the partnership were not told the actual name — Apple Pay — until Mr. Cook announced it on stage. The marketing that the banks had prepared in advance left blank spaces for the name, and for the new Apple devices used in Apple Pay, which the banks also did not know about in advance.

At MasterCard's headquarters in Purchase, N.Y., a marketing team of around 25 people gathered in their own war room, ready to pull the material together once Mr. Cook gave them the final pieces of the puzzle.

In Cupertino, Calif., when Mr. Cook finally did bring up Apple Pay, a JPMorgan employee sitting in the fourth row quickly sent an email to a JPMorgan employee at the financial conference in New York, who then relayed the apple signal to Ms. Lake, the chief financial officer on stage.

"We're delighted to be able to participate," Ms. Lake said.

A version of this article appears in print on 09/12/2014, on page B1 of the NewYork edition with the headline: Banks Did It Apple's Way in Payments by Mobile.

© 2017 The New York Times Company

California Notices

Exhibit 5

FINAL

EMVCo Publishes Technical Framework for its Payment Tokenisation Specification

Technical body calls on industry to engage in its work to create a globally interoperable ecosystem for payment tokenisation

11 March 2014 – The *EMV® Payment Tokenisation Specification - Technical Framework v1.0* has been published by EMVCo. The technical document – which will be of interest to all industry participants including merchants, acquirers, card issuers and new payment entrants engaged in the mobile and digital secure payment ecosystem – is designed to allow market implementers to develop interoperable tokenisation solutions. The global technical body is encouraging interested parties to download the document from the EMVCo website and engage in the ongoing payment tokenisation development activity.

EMVCo, which is collectively owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa, announced that it would expand its scope to lead the payments industry in its work to standardise tokenisation in January 2014. The new specification will help provide the payments community with a consistent, secure and globally interoperable environment to make digital payments when using a mobile handset, tablet, personal computer or other smart device. This will encourage industry efficiencies and security enhancements for digital commerce.

The *EMV Payment Tokenisation Specification - Technical Framework v1.0* describes the payment tokenisation landscape, the types of entities whose participation is key to supporting payment tokenisation, sufficient detail to implement multiple use cases, and the benefits of adopting a unified approach.

From a technical perspective, the document provides an insight into the role the specification will have in facilitating broad-based acceptance of a payment token as a replacement for a traditional card account number. This includes data message formats to ensure the interoperability of tokens and the consistent approach that should be used to route and authenticate a payment token. The framework also explains how security can be improved by limiting payment tokens for use in a specific environment, and how an existing ecosystem can advance to become globally interoperable.

Dave Meadon, current EMVCo Executive Committee Chair, comments: “It is vital that we have a consistent approach to identify and verify a payment token request, which is supported by industry agreed channel controls to manage where and when the payment token can be used. This level of consistency eliminates data vulnerabilities at key points in the transaction, which ultimately enhances security.”

EMVCo has publically released this document to encourage industry adoption of the specification and aid its evolution. Christina Hulka, current EMVCo Board of Managers Chair, adds: “There are a variety of tokenisation systems in existence already. Within EMVCo’s role to facilitate global interoperability and acceptance of secure

payment transactions, our specification work will aim to provide a globally aligned technical framework for payment tokens. This will ensure consistency in data fields and the ability for transactions to gateway successfully throughout the payment ecosystem. By engaging with interested parties we can ensure that industry needs are met across stakeholders. This will enable us to create a standardised, secure and reliable environment across all payment channels."

The new specification from EMVCo will maintain compatibility with the current payment infrastructure and will be complementary to the existing EMV Chip Specifications to ensure consistency across all payment environments. Moving forward, EMVCo will actively solicit Associate, Subscriber and public feedback to support enhancements and inclusion of additional use cases. The specification framework will evolve with industry input collected to broaden its applicability and relevance to marketplace needs.

To fully engage in EMVCo's payment tokenisation activity and provide feedback on global interoperability and security requirements, join EMVCo's established Associates and Subscriber Programme which is open to all industry stakeholders.

Tokenisation is also a key topic that will be covered at the EMV User Meeting, 25-26 June in Kuala Lumpur. This annual interactive forum brings together senior EMVCo representatives, payment card issuers, acquirers, merchants, processors, card and terminal vendors, networks, and their respective associations. Interested parties can register now.

– ENDS –

For further EMVCo media information please contact Sarah Jones / Kirsty Pearson – Tel: +44 1943 468007 or email: sarah@iseepr.co.uk / kirsty@iseepr.co.uk

Notes to Editors:
EMV® is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo.

About EMVCo:
EMVCo is the global technical body that facilitates the worldwide interoperability and acceptance of secure payment transactions by managing and evolving the EMV Specifications and related testing processes. Adoption of EMV Specifications and associated approval and certification processes promotes a unified international payments framework, which supports an advancing range of payment methods, technologies and acceptance environments. The specifications are designed to be flexible and can be adapted regionally to meet national payment requirements and accommodate local regulations.

EMVCo is collectively owned by American Express, Discover, JCB, MasterCard, UnionPay and Visa, and focuses on the technical advancement of the EMV Specifications. To provide all payment stakeholders with a platform to engage in its strategic and technical direction, EMVCo operates an Associates Programme and encourages all interested parties to get involved.

Visit www.emvco.com for further information and join EMVCo on LinkedIn.

Exhibit 6

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CARDWARE INC. *Plaintiff,*	§ §	
v.	§ § §	CASE NO. 2:22-CV-00141-JRG-RSP
SAMSUNG ELECTRONICS CO., LTD. AND SAMSUNG ELECTRONICS AMERICA, INC., *Defendants*.	§ § § §	

STIPULATED PROTECTIVE ORDER

WHEREAS, Plaintiff CardWare Inc. and Defendants Samsung Electronics Co., Ltd and Samsung America, Inc., hereafter referred to as "the Parties," believe that certain information that is or will be encompassed by discovery demands by the Parties involves the production or disclosure of trade secrets, confidential business information, or other proprietary information;

WHEREAS, the Parties seek a protective order limiting disclosure thereof in accordance with Federal Rule of Civil Procedure 26(c):

THEREFORE, it is hereby stipulated among the Parties and ORDERED that:

1. Each Party[1] may designate as confidential for protection under this Order, in whole or in part, any document, information or material that constitutes or includes, in whole or in part, confidential or proprietary information or trade secrets of the Party or a Third Party to whom the Party reasonably believes it owes an obligation of confidentiality with respect to such document, information or material ("Protected Material"). Protected Material shall be

[1] In addition to the named plaintiff(s) and defendant(s) to this lawsuit, "Party" and "Parties" also refers Third Parties (defined below) pursuant to paragraphs 21 and 22 of this Order.

designated by the Party producing it by affixing a legend or stamp on such document, information or material as follows: "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE." The proper designation shall be placed clearly on each page, electronic file, or electronic media containing electronic files of the Protected Material (except deposition and hearing transcripts) for which such protection is sought. For deposition and hearing transcripts, the designation shall be placed on the cover page of the transcript (if not already present on the cover page of the transcript when received from the court reporter) by each attorney receiving a copy of the transcript after that attorney receives notice of the designation of some or all of that transcript under this Order.

2. Any document produced under Patent Rules 2-2, 3-2, and/or 3-4 before issuance of this Order with the designation "CONFIDENTIAL" or "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY" shall receive the same treatment as if designated "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY" under this Order, unless and until such document is redesignated to have a different classification under this Order.

3. With respect to documents, information or material designated "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" ("DESIGNATED MATERIAL"),[2] subject to the provisions herein and unless otherwise stated, this Order governs, without limitation: (a)

[2] The term DESIGNATED MATERIAL is used throughout this Protective Order to refer to the class of materials designated as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSELS EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE"," both individually and collectively.

all documents, electronically stored information, and/or things as defined by the Federal Rules of Civil Procedure; (b) all pretrial, hearing or deposition testimony, or documents marked as exhibits or for identification in depositions and hearings; (c) pretrial pleadings, exhibits to pleadings and other court filings; (d) affidavits; (e) expert reports; and (f) stipulations. All copies, reproductions, extracts, digests and complete or partial summaries prepared from any DESIGNATED MATERIALS shall also be considered DESIGNATED MATERIAL and treated as such under this Order.

4. A designation of Protected Material (i.e., "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE") may be made at any time. Inadvertent or unintentional production of documents, information or material that has not been designated as DESIGNATED MATERIAL shall not be deemed a waiver in whole or in part of a claim for confidential treatment. Any party that inadvertently or unintentionally produces Protected Material without designating it as DESIGNATED MATERIAL may request destruction of that Protected Material by notifying the recipient(s), as soon as reasonably possible after the producing Party becomes aware of the inadvertent or unintentional disclosure, and providing replacement Protected Material that is properly designated. The recipient(s) shall then destroy all copies of the inadvertently or unintentionally produced Protected Materials and any documents, information or material derived from or based thereon.

5. "CONFIDENTIAL" documents, information and material may be disclosed only to the following persons, except upon receipt of the prior written consent of the designating party, upon order of the Court, or as set forth in paragraph 14 herein:

(a) outside counsel of record in this Action for the Parties;

(b) employees of such counsel assigned to and reasonably necessary to assist such counsel in the litigation of this Action;

(c) in-house counsel for the Parties who either have responsibility for making decisions dealing directly with the litigation of this Action, or who are assisting outside counsel in the litigation of this Action and reasonably necessary to assist such counsel in the litigation of this Action;

(d) One (1) designated representative of each of the Parties to the extent reasonably necessary for the litigation of this Action, except that either party may in good faith request the other party's consent to designate one or more additional representatives, the other party shall not unreasonably withhold such consent, and the requesting party may seek leave of Court to designate such additional representative(s) if the requesting party believes the other party has unreasonably withheld such consent;

(e) outside consultants or experts (*i.e.*, not existing employees or affiliates of a Party or an affiliate of a Party) retained for the purpose of this litigation, provided that: (1) such consultants or experts are not presently employed by a Party hereto for purposes other than this Action (not including outside consultants or experts who have also been retained by the same Party for another Action); (2) before access is given, the consultant or expert has completed the Undertaking attached as Appendix A hereto and the same is served upon the producing Party with a current curriculum vitae of the consultant or expert and a list of cases for which the consultant or expert presented testimony (including, but not limited to, written testimony, deposition testimony, and live trial testimony) in the past six years, at least seven (7) days before access to the Protected Material is to be given to that consultant or expert, so that the producing Party may object to and notify the receiving Party in writing that it objects to disclosure of Protected Material to the consultant or expert. The Parties agree to promptly confer and use good faith to resolve any such objection. If the Parties are unable to resolve any objection, the objecting Party may file a motion with the Court within fifteen (15) days of the notice, or within such other time as the Parties may agree, seeking a protective order with respect to the proposed disclosure. The objecting Party shall have the burden of proving the need for a protective order. No disclosure shall occur until all such objections are resolved by agreement or Court order;

(f) independent litigation support services, including persons working for or as court reporters, graphics or design services, jury or trial consulting services, and photocopy, document imaging, and database services retained by counsel and reasonably necessary to assist counsel with the litigation of this Action; and

(g) the Court and its personnel.

6. A Party shall designate documents, information, or material as "CONFIDENTIAL" only upon a good faith belief that the documents, information or material contains confidential or proprietary information or trade secrets of the Party or a Third Party to whom the Party reasonably believes it owes an obligation of confidentiality with respect to such documents, information or material.

7. Documents, information or material produced pursuant to any discovery request in this Action, including but not limited to Protected Material designated as DESIGNATED MATERIAL, shall be used by the Parties only in the litigation of this Action and shall not be used for any other purpose. Any person or entity who obtains access to DESIGNATED MATERIAL or the contents thereof pursuant to this Order shall not make any copies, duplicates, extracts, summaries or descriptions of such DESIGNATED MATERIAL or any portion thereof except as may be reasonably necessary in the litigation of this Action. Any such copies, duplicates, extracts, summaries or descriptions shall be classified DESIGNATED MATERIALS and subject to all of the terms and conditions of this Order.

8. To the extent a producing Party believes that certain Protected Material qualifying to be designated CONFIDENTIAL is so sensitive that its dissemination deserves even further limitation, the producing Party may designate such Protected Material "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or to the extent such Protected Material includes computer source code and/or live data (that is, data as it exists residing in a database or databases) ("Source Code Material"), the producing Party may designate such Protected Material as "HIGHLY CONFIDENTIAL – SOURCE CODE."

9. For Protected Material designated HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY, access to, and disclosure of, such Protected Material shall be limited to

individuals listed in paragraphs 5(a-b) and (e-g).

10. For Protected Material designated "HIGHLY CONFIDENTIAL – SOURCE CODE", the following additional restrictions apply:

(a) Access to a Party's Source Code Material shall be provided only on a "stand-alone" password-protected computer (that is, the computer may not be linked to any network, including a local area network ("LAN"), an intranet or the Internet) ("Source Code Computer").[3] The Source Code Computer shall be connected to (i) a printer, or (ii) a device capable of temporarily storing electronic copies solely for the limited purposes permitted pursuant to paragraphs 10 (h and l) below. Additionally, except as provided in paragraph 10 (l) below, or absent agreement otherwise by the Parties (including the Parties and the producing Party, if different), the Source Code Computer may only be located at the offices of the producing Party's outside counsel. The producing Party's outside counsel shall preserve the Source Code Computer until thirty (30) days after final termination of this Action, including any appeals, and shall be made available to the receiving Party throughout that period upon reasonable notice;

(b) The receiving Party shall make reasonable efforts to restrict its requests for such access to the Source Code Computer to normal business hours, which for purposes of this paragraph shall be 8:00 a.m. through 6:00 p.m. However, upon reasonable notice from the receiving party, the producing Party shall make reasonable efforts to accommodate the receiving Party's request for access to the Source Code Computer outside of normal business hours. The Parties agree to cooperate in good faith such that maintaining the producing Party's Source Code Material at the offices of its outside counsel shall not unreasonably hinder the receiving Party's ability to efficiently and effectively conduct the prosecution or defense of this Action;

(c) The producing Party shall provide the receiving Party with information explaining how to start, log on to, and operate the Source Code Computer in order to access the produced Source Code Material on the Source Code Computer;

(d) The producing Party will produce Source Code Material in computer searchable format on the Source Code Computer. The receiving Party may request software tools for viewing and searching the Source Code Material be installed on the computer, provided, however, that such review of the Source Code Material are in compliance with all of the terms, conditions, and protections herein. The receiving

[3] A second Source Code Computer may be provided at the same location as the Source Code Computer at a receiving Party's request to accommodate simultaneous review by multiple reviewers. All restrictions described herein that are applicable to the Source Code Computer shall apply to said second Source Code Computer. The parties will work in good faith to select a location for the source code computer(s) that is convenient for all parties, considering the location of Defendants' law firms' offices and the location of Plaintiff's expert(s).

Party must provide the producing Party with the CD or DVD containing such licensed software tool(s), or a link to a website where the software may be downloaded for installation together with any necessary license, at least five (5) business days in advance of the date upon which the receiving Party wishes to have the software tools available for use on the computer. Should the producing Party have any concerns about the requested tool, such as that they are used for things other than reviewing and searching source code or not commonly accepted in the industry, the Parties shall meet and confer in good faith to resolve any such concerns. Otherwise, assuming the above conditions are met, the producing Party shall install the requested software tools on the Source Code Computer;

(e) Access to Protected Material designated HIGHLY CONFIDENTIAL – SOURCE CODE shall be limited to outside counsel and up to three (3) outside consultants or experts[4] (*i.e.*, not existing employees or affiliates of a Party or an affiliate of a Party) retained for the purpose of this litigation and approved to access such Protected Materials pursuant to paragraph 5(e) above. A receiving Party may include excerpts of Source Code Material in a pleading, exhibit, expert report, discovery document, deposition transcript, or other Court document ("Source Code Documents"), provided that the Source Code Documents are appropriately marked under this Order, restricted to those who are entitled to have access to them as specified herein, and, if filed with the Court, filed under seal in accordance with the Court's rules, procedures and orders;

(f) To the extent portions of Source Code Material are quoted in a Source Code Document, either (1) the entire Source Code Document will be stamped and treated as HIGHLY CONFIDENTIAL – SOURCE CODE or (2) those pages containing quoted Source Code Material will be separately stamped and treated as HIGHLY CONFIDENTIAL – SOURCE CODE;

(g) Except as set forth in paragraphs 10(j) and (l) below, no electronic copies of Source Code Material shall be made without prior written consent of the producing Party, except as necessary to create documents which, pursuant to the Court's rules, procedures and order, must be filed or served electronically;

(h) The receiving Party shall be permitted to make a reasonable number of printouts and photocopies of Source Code Material, all of which shall be designated and clearly labeled "RESTRICTED CONFIDENTIAL SOURCE CODE," and the receiving Party shall maintain a log of all such files that are printed or photocopied;

[4] For the purposes of this paragraph, an outside consultant or expert is defined to include the outside consultant's or expert's direct reports and other support personnel, such that the disclosure to a consultant or expert who employs others within his or her firm to help in his or her analysis shall count as a disclosure to a single consultant or expert.

(i) Should such printouts or photocopies be transferred back to electronic media, such media shall be labeled "HIGHLY CONFIDENTIAL – SOURCE CODE" and shall continue to be treated as such;

(j) For depositions, copies of Source Code Material that are marked as deposition exhibits shall not be provided to the Court Reporter or attached to deposition transcripts. Rather, the deposition record will identify the exhibit by its production numbers. All paper copies of Source Code Material brought to a deposition by the receiving Party shall be securely retained by the receiving Party's outside counsel or turned over to the producing Party's outside counsel immediately following the close of the deposition for secure destruction in a timely manner. However, this subparagraph 10(j) shall not apply to any page or portion of Source Code Material marked or altered during the deposition, and only those marked or altered pages or portions shall be retained by the Court Reporter and provided to the Parties;

(k) If the receiving Party's outside counsel, consultants, or experts obtain printouts or photocopies of Source Code Material, the receiving Party shall ensure that such outside counsel, consultants, or experts keep the printouts or photocopies in a secured locked area in the offices of such outside counsel, consultants, or expert, or similarly secure location. The receiving Party may also temporarily keep the printouts or photocopies at: (i) the Court for any proceedings(s) relating to the Source Code Material, for the dates associated with the proceeding(s); (ii) the sites where any deposition(s) relating to the Source Code Material are taken, for the dates associated with the deposition(s); and (iii) any intermediate location reasonably necessary to transport the printouts or photocopies (*e.g.*, a hotel prior to a Court proceeding or deposition)

(l) A producing Party's Source Code Material may only be transported by the receiving Party at the direction of a person authorized under paragraph 10(e) above to another person authorized under paragraph 10(e) above, on paper or removable electronic media (*e.g.*, a DVD, CD-ROM, or flash memory "stick") via hand carry, Federal Express or other similarly reliable courier. Source Code Material may not be transported or transmitted electronically over a network of any kind, including a LAN, an intranet, or the Internet. Source Code Material may only be transported electronically for the purpose of Court proceeding(s) or deposition(s) as set forth in paragraph 10(k) above and is at all times subject to the transport restrictions set forth herein. But, for those purposes only, the Source Code Materials may be loaded onto a stand-alone computer; and

(m) All persons who will review a producing Party's Source Code Material on the Source Code Computer on behalf of a receiving Party, including members of a receiving Party's outside law firm, shall be identified in writing to the producing Party at least five (5) days in advance of the first time that such person reviews Source Code Material on the Source Code Computer. Such identification shall be in addition to any other disclosure required under this Order. All persons viewing Source Code Material on the Source Code Computer shall sign on each day they view Source Code Material a log that will include the names of persons who view

the Source Code Material on the Source Code Computer and when they enter and depart the Source Code Review Room. Proper identification of all authorized persons shall be provided prior to any access to the Source Code Review Room or the Source Code Computer. Proper identification requires showing, at a minimum, a photo identification card sanctioned by the government of any State of the United States, by the government of the United States, or by the nation state of the authorized person's current citizenship. Access to the Source Code Review Room or the Source Code Computer may be denied, at the discretion of the producing Party, to any individual who fails to provide proper identification;

11. Absent written consent from the producing Party, any individual who receives access to HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES ' ONLY and/or HIGHLY CONFIDENTIAL – SOURCE CODE information (collectively "HIGHLY SENSITIVE MATERIAL") shall not prepare, prosecute, supervise, or assist in the preparation or prosecution of any patent application pertaining to the field of the invention of any patent-in-suit on behalf of the receiving Party or its acquirer, successor, predecessor, or other affiliate during the pendency of this Action and for one year after its conclusion, including any appeals. To ensure compliance with the purpose of this provision, each Party shall create an "Ethical Wall" between those persons with access to HIGHLY SENSITIVE MATERIAL and any individuals who, on behalf of the Party or its acquirer, successor, predecessor, or other affiliate, prepare, prosecute, supervise or assist in the preparation or prosecution of any patent application pertaining to the field of invention of any patent-in-suit. This Prosecution Bar shall begin when HIGHLY SENSITIVE MATERIAL is first reviewed by the affected individual.

12. Nothing in this Order shall require production of documents, information or other material that a Party contends is protected from disclosure by the attorney-client privilege, the work product doctrine, or other privilege, doctrine, or immunity. The Court's Discovery Order

shall govern issues related to attorney-client privilege, the work product doctrine, or other privilege, doctrine, or immunity.

13. There shall be no disclosure of any DESIGNATED MATERIAL by any person authorized to have access thereto to any person who is not authorized for such access under this Order. The Parties are hereby ORDERED to safeguard all such documents, information and material to protect against disclosure to any unauthorized persons or entities.

14. Nothing contained herein shall be construed to prejudice any Party's right to use any DESIGNATED MATERIAL in taking testimony at any deposition or hearing or in participating in mediation or settlement discussions provided that the DESIGNATED MATERIAL is only disclosed to a person(s) who is: (i) eligible to have access to the DESIGNATED MATERIAL by virtue of his or her employment with the designating party, (ii) identified in the DESIGNATED MATERIAL as an author, addressee, or copy recipient of such information, (iii) although not identified as an author, addressee, or copy recipient of such DESIGNATED MATERIAL, has, in the ordinary course of business, seen such DESIGNATED MATERIAL, (iv) a current or former officer, director or employee of the producing Party or a current or former officer, director or employee of a company affiliated with the producing Party; (v) counsel for a Party, including outside counsel and in-house counsel (subject to paragraph 9 of this Order); (vi) an independent contractor, consultant, and/or expert retained for the purpose of this litigation; (vii) court reporters and videographers; (viii) the Court; (ix) one (1) designated representative of a Party with mediation and/or settlement authority for that Party, however, disclosure to that designated representative is limited only to DESIGNATED MATERIAL necessary for that designated representative to participate in mediation or to exercise settlement

authority, shall not include any HIGHLY CONFIDENTIAL – SOURCE CODE material and shall only be disclosed after the procedures set forth in paragraph 15; or (x) other persons entitled hereunder to access to DESIGNATED MATERIAL. DESIGNATED MATERIAL shall not be disclosed to any other persons unless prior authorization is obtained from counsel representing the producing Party or from the Court.

15. Any Party that intends to disclose non-technical DESIGNATED MATERIAL to a designated representative, as set forth in paragraph 14(ix), shall notify the producing Party in writing requesting approval to disclose such information not less than fourteen (14) days before the intended disclosure. The producing Party shall have three (3) business days to object to the disclosure and/or provide any proposed redactions. Such objections and redactions shall be limited to those that the producing Party believes in good faith would cause it competitive harm if disclosed. The Parties shall then meet and confer, if necessary, within three (3) business days to discuss the producing Party's objections and/or proposed redactions and attempt in good faith to resolve any disputes.

16. Parties may, at the deposition or hearing or within thirty (30) days after receipt of a deposition or hearing transcript, designate the deposition or hearing transcript or any portion thereof as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" pursuant to this Order. Access to the deposition or hearing transcript so designated shall be limited in accordance with the terms of this Order. Until expiration of the 30-day period, the entire deposition or hearing transcript shall be treated as HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY.

17. Any DESIGNATED MATERIAL that is filed with the Court shall be filed under seal and

shall remain under seal until further order of the Court. The filing party shall be responsible for informing the Clerk of the Court that the filing should be sealed and for placing the legend "FILED UNDER SEAL PURSUANT TO PROTECTIVE ORDER" above the caption and conspicuously on each page of the filing. Exhibits to a filing shall conform to the labeling requirements set forth in this Order. If a pretrial pleading filed with the Court, or an exhibit thereto, discloses or relies on confidential documents, information or material, such confidential portions shall be redacted to the extent necessary and the pleading or exhibit filed publicly with the Court.

18. The Order applies to pretrial discovery. Nothing in this Order shall be deemed to prevent the Parties from introducing any DESIGNATED MATERIAL into evidence at the trial of this Action, or from using any information contained in DESIGNATED MATERIAL at the trial of this Action, subject to any pretrial order issued by this Court.

19. A Party may request in writing to the other Party that the designation given to any DESIGNATED MATERIAL be modified or withdrawn. If the designating Party does not agree to redesignation within ten (10) days of receipt of the written request, the requesting Party may apply to the Court for relief. Upon any such application to the Court, the burden shall be on the designating Party to show why its classification is proper. Such application shall be treated procedurally as a motion to compel pursuant to Federal Rules of Civil Procedure 37, subject to the Rule's provisions relating to sanctions. In making such application, the requirements of the Federal Rules of Civil Procedure and the Local Rules of the Court shall be met. Pending the Court's determination of the application, the designation of the designating Party shall be maintained.

20. Each outside consultant or expert to whom DESIGNATED MATERIAL is disclosed in

accordance with the terms of this Order shall be advised by counsel of the terms of this Order, shall be informed that he or she is subject to the terms and conditions of this Order, and shall sign an acknowledgment that he or she has received a copy of, has read, and has agreed to be bound by this Order. A copy of the acknowledgment form is attached as Appendix A.

21. To the extent that any discovery is taken of persons who are not Parties to this Action ("Third Parties") and in the event that such Third Parties contended the discovery sought involves trade secrets, confidential business information, or other proprietary information, then such Third Parties may agree to be bound by this Order.

22. To the extent that discovery or testimony is taken of Third Parties, the Third Parties may designate as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "RESTRICTED CONFIDENTIAL SOURCE CODE" any documents, information or other material, in whole or in part, produced or given by such Third Parties. The Third Parties shall have ten (10) days after production of such documents, information or other materials to make such a designation. Until that time period lapses or until such a designation has been made, whichever occurs sooner, all documents, information or other material so produced or given shall be treated as "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY" in accordance with this Order.

23. Within thirty (30) days of final termination of this Action, including any appeals, all DESIGNATED MATERIAL, including all copies, duplicates, abstracts, indexes, summaries, descriptions, and excerpts or extracts thereof (excluding excerpts or extracts incorporated into any privileged memoranda of the Parties and materials which have been admitted into evidence in this Action), shall at the producing Party's election either be returned to the

producing Party or be destroyed. The receiving Party shall verify the return or destruction by affidavit furnished to the producing Party, upon the producing Party's request.

24. The failure to designate documents, information or material in accordance with this Order and the failure to object to a designation at a given time shall not preclude the filing of a motion at a later date seeking to impose such designation or challenging the propriety thereof. The entry of this Order and/or the production of documents, information and material hereunder shall in no way constitute a waiver of any objection to the furnishing thereof, all such objections being hereby preserved.

25. Any Party (including any Third Party that has produced DESIGNATED MATERIAL) knowing or believing that any other Party is in violation of or intends to violate this Order and has raised the question of violation or potential violation with that Party and has been unable to resolve the matter by agreement may move the Court for such relief as may be appropriate in the circumstances. Pending disposition of the motion by the Court, the Party alleged to be in violation of or intending to violate this Order shall discontinue the performance of and/or shall not undertake the further performance of any action alleged to constitute a violation of this Order.

26. Production of DESIGNATED MATERIAL by each of the Parties or by any Third Parties shall not be deemed a publication of the documents, information and material (or the contents thereof) produced so as to void or make voidable whatever claim the Parties may have as to the proprietary and confidential nature of the documents, information or other material or its contents.

27. Nothing in this Order shall be construed to effect an abrogation, waiver or limitation of any kind on the rights of each of the Parties to assert any applicable discovery or trial privilege.

28. Each of the Parties shall also retain the right to file a motion with the Court (a) to modify this Order to allow disclosure of DESIGNATED MATERIAL to additional persons or entities if reasonably necessary to prepare and present this Action and (b) to apply for additional protection of DESIGNATED MATERIAL.

SIGNED this 21st day of October, 2022.

ROY S. PAYNE
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

CARDWARE INC. *Plaintiff,* v. SAMSUNG ELECTRONICS CO., LTD. AND SAMSUNG ELECTRONICS AMERICA, INC., *Defendants*.	§ § § § § § § § § § §	CASE NO. 2:22-cv-00141-JRG-RSP

APPENDIX A
UNDERTAKING OF EXPERTS OR CONSULTANTS REGARDING PROTECTIVE ORDER

I,_____, declare that:

1. My address is_____.

   My current employer is_____.

   My current occupation is_____.

2. I have received a copy of the Protective Order in this action. I have carefully read and understand the provisions of the Protective Order.

3. I will comply with all of the provisions of the Protective Order. I will hold in confidence, will not disclose to anyone not qualified under the Protective Order, and will use only for purposes of this action any information designated as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" that is disclosed to me.

4. Promptly upon termination of this action, I will return all documents and things designated as "CONFIDENTIAL," "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL EYES' ONLY," or "HIGHLY CONFIDENTIAL – SOURCE CODE" that came into my possession, and all documents and things that I have prepared relating thereto, to the outside counsel for the party by whom I am employed.

5. I hereby submit to the jurisdiction of this Court for the purpose of enforcement of the Protective Order in this action.

I declare under penalty of perjury that the foregoing is true and correct.

Signature

_____

Date

_____