Attachment A

DEFINITIONS & ADDITIONAL INSTRUCTIONS

A. "**Breach**" shall mean an incident in which sensitive, protected or confidential data has potentially been viewed, taken, or used by an unauthorized individual.

B. **"Acquiring Bank" or "Acquirer"** shall mean (a) a bank, financial institution or other company, including its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, that acquires and processes payment card transactions from merchants; and (b) any payment processors, independent sales organizations, membership service providers or other third parties contracted by a bank or financial institution to provide merchant acquiring or payment processing services.

C. **"Attestation of Compliance" or "AOC"** shall mean a form for merchants and service providers to attest to the results of a PCI DSS Compliance Assessment, as documented in the Report on Compliance.

D. "**Company**" shall mean [Company], its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, members, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

E. "**Data Security Forensic Audit Services**" shall mean services related to examining a computer network following a Breach or other security incident in order to determine the cause and extent of the Breach or other security incident.

F. "**Data Security Services**" shall mean services related to the security of computer networks, including audits, assessments, programs, monitoring services, or the establishment of a computer network.

G. "**Identify**" shall be construed to require identification of (a) natural persons by name, title, present business affiliation, present business address and telephone number, or if a present business affiliation or present business address is not known, the last known business and home addresses; and (b) businesses or other organizations by name, address, identities of natural persons who are officers, directors or managers of the business or organization, and contact persons, where applicable.

H. **"Issuing Bank"** shall mean a bank, financial institution or other company, including its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, that issues payment cards to cardholders.

I. "**Order"** shall mean the Order, including the attached Resolution, Specifications, and Attachment.

J. **"Payment Card Network"** shall mean a company, its wholly owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, that facilitates the electronic transfer of data and funds among merchants, Acquiring Banks, and Issuing Banks when payment cards are used to make purchases, including but not limited to Visa Inc., MasterCard, American Express, and Discover Financial Services.

K. "**PCI DSS Compliance Assessments**" or "**Compliance Assessments**" shall mean an onsite assessment performed by a Qualified Security Assessor to determine whether a business has complied with the Payment Card Industry Data Security Standard.

L. "**Qualified Security Assessor**" or "**QSA**" shall mean a company or individual that has been qualified by the PCI Security Standards Council to perform Compliance Assessments.

M. "**Report on Compliance**" or **"ROC"** shall mean a report documenting detailed results from a Compliance Assessment.

N. "**You**" and "**your**" shall mean the person or entity to whom this CID is issued and includes the "Company."

O. **Meet and Confer:** You are encouraged to contact **David Lincicum** at **(202) 326-2773** or **Ben Rossen** at **(202) 326-3679** as soon as possible to schedule a meeting (telephonic or in person) in order to confer regarding your response.

P. **Modification of Specifications:** If you believe that the scope of the required search or response for any specification can be narrowed consistent with the Commission's need for documents or information, you are encouraged to discuss such possible modifications, including any modifications of definitions and instructions, with the Commission counsel named above.

Q. **Electronic Submission of Documents:** See the attached "Federal Trade Commission, Bureau of Consumer Protection Production Requirements," which details all requirements for submission of information, generally requiring that files be produced in native form and specifying the metadata to be produced. As noted in the attachment, some items require discussion with the FTC counsel **prior to** production, which can be part of the general "Meet and Confer" described above. If you would like to arrange a separate discussion involving persons specifically familiar with your electronically stored information (ESI) systems and methods of retrieval, make those arrangements with FTC counsel when scheduling the general meet and confer discussion.

R. **Applicable Time Period**: Unless otherwise directed in the specifications, the applicable time period for the request shall be from **January 1, 2013 until the date of full and complete compliance with this Order.**

S. **Document Production**: Because postal delivery to the Commission is subject to delay due to heightened security precautions, please use a courier service such as Federal Express or UPS.

T. **Production of Copies**: Copies of marketing materials and advertisements shall be produced in color, and copies of other materials shall be produced in color if necessary to interpret them or render them intelligible.

U. **Sensitive Personally Identifiable Information**: If any material called for by these requests contains sensitive personally identifiable information or sensitive health information of any individual, please contact us before sending those materials to discuss whether it would be appropriate to redact the sensitive information. If that information will not be redacted, contact us to discuss encrypting any electronic copies of such material with encryption software such as SecureZip and provide the encryption key in a separate communication.

For purposes of these requests, sensitive personally identifiable information includes: an individual's Social Security number alone; or an individual's name or address or phone number in combination with one or more of the following: date of birth; Social Security number; driver's license number or other state identification number or a foreign country equivalent; passport number; financial account number; credit card number; or debit card number. Sensitive health information includes medical records and other individually identifiable health information relating to the past, present, or future physical or mental health or conditions of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Federal Trade Commission, Bureau of Consumer Protection Production Requirements

Submit all documents according to the instructions, below. Some instructions require **discussion with FTC counsel prior to production**, which can be part of a general "Meet and Confer" between the parties or a separate discussion involving persons specifically familiar with your electronically stored information (ESI) systems and methods of retrieval.

Types of Files

1. Native or Near-Native Files

    a. Whenever possible, produce responsive ESI in its native form; that is, in the form in which the information was customarily created, used and stored by the native application employed by the producing party in the ordinary course of business (i.e., .doc, .xls, .ppt, .pdf).

    b. If production of an ESI item in its native form is infeasible, it may be produced in a near-native form (i.e., there is not a material loss of content, structure or functionality as compared to the native form) that the FTC agrees to prior to production.

    c. Native files containing embedded files must have those files extracted, produced in their native form in accordance with #1.a., and have the parent/child relationship identified in the accompanying production metadata.

2. Databases

    a. Microsoft Access databases may be produced in either .mdb or .accdb format.

    b. Discuss all other database formats with the FTC prior to production.

3. Multimedia

    a. Multimedia files (i.e., audio, video) may be produced in .mp3 or .mp4 formats.

    b. Discuss production of multimedia (i.e., audio, video) in other file formats with the FTC prior to production.

4. Discuss production of instant messages, CRM, proprietary applications, and any other type of ESI not specifically referenced in #1, 2, or 3 with the FTC prior to production.

5. Hard Copy Documents

    a. Scan in an electronic format documents stored in hard copy in the ordinary course of business.
    b. Produce scanned documents as 300 DPI individual multi-page PDFs per document. For marketing materials and where necessary to interpret documents or render them intelligible, submit documents in color.

    c. Produce scanned documents with embedded searchable text.

    d. Produce hard copy documents in the order in which they appear in your files and without being manipulated or otherwise rearranged.

    e. Treat documents kept in folders or binders as family members. Scan the cover of a binder or folder separately and have it serve as the parent document. Scan each document within a folder or binder as an individual document and have it serve as a child to the parent folder or binder.

6. Redacted Documents

    a. Produce ESI requiring redaction in a near native searchable PDF format.

    b. Produce redacted documents as individual multi-page PDFs per document.

    c. Produce redacted documents with embedded searchable text.

    d. If hard copy documents require redaction, follow all requirements laid out in #5.

De-duplication, Email Threading, and Passwords

7. De-duplication

    a. De-duplication based on MD5 or SHA-1 hash value may be conducted within a custodian's set of files without FTC approval so long as the FTC is notified of the intent to de-duplicate prior to production.

    b. Discuss de-duplication of any other scope or means with the FTC prior to production.

8. Use of email threading software must be discussed with the FTC prior to production.

9. For password protected files, remove their passwords prior to production. If password removal is not possible, provide a cross reference file including original filename, production filename, and the respective password.

Production Metadata

10. Family Relationships: Regardless of form of production, preserve the parent/child relationship in all files as follows:

    a. Produce attachments as separate documents and number them consecutively to the parent file.

    b. Complete the ParentID metadata field for each attachment.

11. Document Numbering and File Naming

    a. Each document must have a unique document identifier ("DOCID") consisting of a prefix and 7-digit number (e.g., ABC0000001) as follows:
        i. The prefix of the filename must reflect a unique alphanumeric designation, not to exceed seven (7) characters identifying the producing party. This prefix must remain consistent across all productions.
        ii. The next seven (7) digits must be a unique, consecutive numeric value assigned to the item by the producing party. Pad this value with leading zeroes as needed to preserve its 7-digit length.
        iii. Do not use a space to separate the prefix from numbers.

    b. Name each native or near native file with its corresponding DOCID number and appropriate file extension (e.g., ABC0000001.doc).

12. Load File Format

    a. Produce metadata in a delimited text file (.DAT) for each item included in the production. The first line of the delimited text file must contain the field names. Each subsequent line must contain the metadata for each produced document.

    b. Use these delimiters in the delimited data load file:

Description	Symbol	ASCII Code
Field Separator	¶	020
Quote Character	Þ	254
New Line	®	174
Multiple Field Entries	;	059

13. The following chart describes the required metadata for native, scanned, and redacted documents. If you want to submit additional metadata, discuss with the FTC prior to production.

Production Metadata				
Field Name	**Native**	**Scanned**	**Redacted**	**Format**
DOCID	Y	Y	Y	Alphanumeric (*see* #11 above)
PARENTID	Y	Y	Y	Alphanumeric

NATIVELINK	Y	Y	Y	Alphanumeric
CUSTODIAN	Y	Y	Y	Alphanumeric
RESPSPEC	Y	Y	Y	Alphanumeric (question # record responds to)
ORIGFILENAME	Y		Y	Alphanumeric
ORIGPATH	Y		Y	Alphanumeric
CONFIDENTIAL	Y	Y	Y	Boolean - Y/N
HASH	Y	Y	Y	Alphanumeric
From			Y	Alphanumeric
To			Y	Alphanumeric
CC			Y	Alphanumeric
BCC			Y	Alphanumeric
EmailSubject			Y	Alphanumeric
DateSent			Y	MM/DD/YYYY HH:MM:SS AM/PM
DateRcvd			Y	MM/DD/YYYY HH:MM:SS AM/PM
Author			Y	Alphanumeric
Subject			Y	Alphanumeric
DateCreated			Y	MM/DD/YYYY HH:MM:SS AM/PM
DateLastMod			Y	MM/DD/YYYY HH:MM:SS AM/PM

Production Media

14. Prior to production, scan all media and data contained therein for viruses and confirm the media and data is virus free.

15. For productions smaller than 50 GB, the FTC can accept electronic file transfer via FTC hosted secure file transfer protocol. Contact the FTC to request this option. The FTC cannot accept files via Dropbox, Google Drive, or other third-party file transfer sites.

16. Use the least amount of media necessary for productions. Acceptable media formats are optical discs (CD, DVD), flash drives, and hard drives. Format all media for use with Windows 7.

17. Data encryption tools may be employed to protect privileged or other personal or private information. Discuss encryption formats with the FTC prior to production. Provide encryption passwords in advance of delivery, under separate cover.

18. Mark the exterior of all packages containing electronic media sent through the U.S. Postal Service or other delivery services as follows:

MAGNETIC MEDIA – DO NOT X-RAY
MAY BE OPENED FOR POSTAL INSPECTION.

19. Provide a production transmittal letter with all productions which includes:
    a. A unique production number (e.g., Volume I).
    b. Date of production.

c. The numeric range of documents included in the production.
The number of documents included in the production.