United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Hannaford Brothers Co.
145 Pleasant Hill Road
Scarborough, Maine 04074
Attn: Ronald C. Hodge, CEO

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

□ You are required to appear and testify.

LOCATION OF HEARING	YOUR APPEARANCE WILL BE BEFORE
	DATE AND TIME OF HEARING OR DEPOSITION

☒ You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

☒ You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

NOV 3 0 2010

3. SUBJECT OF INVESTIGATION

See attached resolutions

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN Alain Sheer/Loretta Garrison Bureau of Consumer Protection Federal Trade Commission 601 New Jersey Avenue, NW Washington D.C. 20580	5. COMMISSION COUNSEL Alain Sheer, Bureau of Consumer Protection Federal Trade Commission 601 New Jersey Avenue, NW Washington D.C. 20580 202.326.3321
DATE ISSUED 11/2/10	COMMISSIONER'S SIGNATURE

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's *Rules of Practice* is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's *Rules of Practice* require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature ______________________

Title ______________________

Sworn to before me this day

______________________ ________

____
Notary Public

____

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
Pamela Jones Harbour
William E. Kovacic
J. Thomas Rosch

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN A NON-PUBLIC INVESTIGATION OF UNNAMED PERSONS, PARTNERSHIPS, CORPORATIONS, OR OTHERS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF TITLE V OF THE GRAMM-LEACH-BLILEY ACT AND/OR SECTION 5 OF THE FTC ACT

File No. 002 3284

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others have engaged in or are engaging in acts or practices in violation of Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827 and/or Section 5 of the FTC Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory process available to it be used in connection with this investigation for a period not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five (5) year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five (5) year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five (5) year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; and FTC Procedures and Rules of Practice, 16 C.F.R. § 1.1 *et seq.*, and supplements thereto.

By direction of the Commission.

Donald S. Clark

Donald S. Clark
Secretary

Issued: July 16, 2009

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS:

Robert Pitofsky, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION INTO THE ACTS AND PRACTICES OF UNNAMED PERSONS, PARTNERSHIPS AND CORPORATIONS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF 15 U.S.C. § 1681 ET SEQ. AND/OR 15 U.S.C. § 45

File No. 992-3120

Nature and Scope of Investigation:

An investigation to determine whether persons, partnerships or corporations may be engaging in, or may have engaged in, acts or practices in violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and/or Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended, relating to information furnished to consumer reporting agencies, maintained in the files of consumer reporting agencies, or obtained as a consumer report from a consumer reporting agency. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. § § 46, 49, 50 and 57b-1, as amended; FTC Procedures and Rules of Practices 16 C.F.R. 1.1 et seq. and supplements thereto.

Title VI of the Consumer Credit Protection Act, Section 621, 15 USCA § 1681s.

By direction of the Commission.

Donald S. Clark

Donald S. Clark
Secretary

Dated: April 15, 1999

FIRST CIVIL INVESTIGATIVE DEMAND
TO HANNAFORD BROTHERS CO.

DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

A. **"Acquiring bank"** shall mean a bank or financial institution that provides accounts to merchants that are used in processing and settling payment card transactions for merchants.

B. **"And,"** as well as **"or,"** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in the Schedule all information that otherwise might be construed to be outside the scope of the specification.

C. **"Any"** shall be construed to include **"all,"** and **"all"** shall be construed to include the word **"any."**

D. **"The breach"** shall mean the unauthorized connection to and installation of hacker tools on Hannaford, Sweetbay, or Shop 'n Save computer networks, regarding which Hannaford was alerted on February 27, 2008 and which it disclosed publicly on March 17, 2008.

E. **"CID"** shall mean this Civil Investigative Demand, the attached Resolution, and the accompanying Schedule, including the Definitions, Instructions, and Specifications.

F. **"Document"** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book or label. "Document" shall also include Electronically Stored Information.

G. **"Electronically Stored Information" or "ESI"** shall mean the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created or stored information, including but not limited to electronic mail, instant messaging, videoconferencing, and direct connections or other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, cell phones, Blackberry, PDA, or other storage media, and such technical assistance or instructions as will transform such ESI into a reasonably usable form.

H. **"Each"** shall be construed to include **"every,"** and **"every"** shall be construed to include **"each."**

I. **"FTC"** or **"Commission"** shall mean the Federal Trade Commission.

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

K. **"Identify"** or **"the identity of"** 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.

L. **"Payment cards"** shall mean credit cards, debit cards, electronic benefit transfer cards, gift cards, stored-value cards, insurance cards, or any other cards presented by a consumer to purchase goods or services or obtain cash.

M. **"Personal Information"** shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a date of birth; (f) payment card information, including card number, expiration date, electronic security code, and data stored on the magnetic stripe of a card; (g) a Personal Identification Number for a payment card; (h) a government-issued identification number, such as a driver's license, military identification, passport, or Social Security number; (i) an employee identification number; (j) bank routing, account, and check numbers; (k) personal check cashing history; (l) prescription information, such as medication and dosage, prescribing physician name, address, and telephone number, health insurer name, and insurance account and policy numbers; (m) pharmacy information; (n) income, employment, retirement, disability, and medical records; (o) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; and (p) any information that is combined with any of (a) through (o) above. For the purpose of this provision, a "consumer" shall include an "employee" and an individual seeking to become an employee, where "employee" shall mean an agent, servant, salesperson, associate, independent contractor, and other person directly or indirectly under the control of Hannaford, Sweetbay, or Shop 'n Save.

N. **"Pharmacy Information"** shall mean information related to pharmacy transactions, reports or files on controlled substances, pharmacy customer files, flexible spending accounts or other similar customer accounts, and "protected health information," as that term is defined in 45 CFR § 160.103.

O. **"POS network"** shall mean the computers, servers, devices, and applications used at the point of sale to: (a) process and complete consumer purchases, including, but not limited to, purchases made with payment cards, checks, and cash, and (b) provide other services, such as cashing personal and payroll checks.

P. **"Referring to"** or **"relating to"** shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

Q. **"Security practice"** shall mean security procedures, practices, policies, and defenses.

R. **"Shop 'n Save"** shall mean the independently owned food retailers in Maine, New Hampshire, and New York to which Hannaford sells groceries at wholesale and to which it provides payment transaction processing.

S. **"Sweetbay"** shall mean Hannaford's sister company, Sweetbay Supermarket, which operates retail food stores in Florida.

T. **"You"** and **"Your"** shall mean the entity to which this CID is issued and includes Hannaford.

INSTRUCTIONS

A. **Sharing of Information:** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11(c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. **Meet and Confer:** You must contact Alain Sheer at (202) 326-3221 as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your production of documents and information.

C. **Applicable time period:** Unless otherwise directed in the specifications, the applicable time period for the CID shall be from **January 1, 2007 until the date of full and complete compliance with this CID.** These specifications shall be deemed continuing in nature so as to require production of all documents responsive to any specification included in this CID that you have created, received, or discovered until forty-five days prior to the date of the Company's full compliance with this CID.

D. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;

2. the names, addresses, positions, and organizations of all authors and recipients of the item; and

3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

E. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. *See* 15 U.S.C. § 50; *see also* 18 U.S.C. §§ 1505, 1519. If, for any specification, there are documents that would be responsive to this CID, but they were destroyed, mislaid, transferred, deleted, altered, or over-written, describe the date and the circumstances.

F. **Petitions to Limit or Quash:** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

G. **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 Alain Sheer at (202) 326-3321. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

H. **Certification:** A responsible corporate officer shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

I. **Scope of Search:** This CID covers documents and information in your possession or under your actual or constructive custody or control including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, consultants, contractors, third-party providers, vendors, directors, officers, employees, and other agents, whether or not such documents were received from or disseminated to any person or entity.

J. **Document Production:** You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Alain Sheer, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Mail Stop NJ-8100, Washington, D.C. 20580. 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. Notice of your intended method of production shall be given by mail or telephone to Alain Sheer at (202) 326-3321 at least five days prior to the return date.

K. **Document Identification:** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. Documents should be produced in the order in which they appear in your files and without being shuffled or otherwise rearranged; if documents are removed from their original folders, binders, covers, or containers in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, or container from which such documents came. In addition, number by page all documents in your submission and indicate the total number of documents in your submission. Also number all media in your submission which contain ESI and indicate the contents of the media. For media containing ESI, identify the file path where each of the individual files is located.

L. **Production of Copies:** Unless otherwise stated, legible photocopies may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of original documents may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request. 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.

M. **Submission of Electronic Data/Forms of Production**

1. The following data delivery standards outline the technical requirements for electronic document productions produced to the Federal Trade Commission. Any proposed formats other than what is listed below (including databases) should not be produced with out discussion and approval from the Litigation Support Manager of the Bureau of Consumer Protection. Submissions should be organized by custodian unless otherwise instructed. The FTC uses Concordance 9.x and Opticon 4.x to review their electronic document collections.

2. General Guidelines

a. Documents stored in electronic or hard copy formats shall be produced as kept in the usual course of business; the FTC prefers electronically formatted productions provided that such electronic copies are true, correct, and complete copies of the original documents.

b. Documents shall be produced in a complete form, un-redacted unless privileged, and in the order which they are kept in the Company's files in the usual course of business, inclusive of staples, clips and/or bound sections so as "re-produce" the original document delineations. For example:

   i) If in their original condition hard copy documents were stapled, clipped, or otherwise fastened together or maintained in file folders, binders, covers, or containers, they shall be reproduced in such form, and any documents that must be removed form their original folders, binders, covers, or containers in order to be produced shall be identified in a manner so as to clearly specify the folder, binder, cover or container from which such documents came.

   ii) If in their original condition electronic documents were kept in folders or otherwise organized (such as on a shared network drive or in an email program), they shall be produced in such form and information shall be produced so as to clearly specify the folder for organization format.

c. Documents shall be produced in color where necessary to interpret the document (if the coloring of any document communicates any substantive information, of if black-and-white photocopying of conversion to TIFF format of any document (e.g., a chart or graph), makes any substantive information contained in the document unintelligible, the Company shall submit the original document, a like-colored photocopy, or a JPEG format image).

d. If any de-duplication or email threading software or services are used when collecting or reviewing information that is stored in the Company's computer systems or electronic storage media, or the Company's computer systems contain or utilize such software, the Company shall contact Alain Sheer at (202) 326-3321.

e. A network diagram(s) depicting the Company's computer network(s) shall be produced. Typically, a network diagram will include a visual schematic identifying computer devices and communication devices within the network.

f. Microsoft Access, SQL, other databases, Microsoft Excel, and PowerPoint files shall be produced in native format with extracted text and metadata.

All database productions shall include a database schema that defines the tables, the fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, Java, XML schemas, and other elements.

g. Data compilations in Microsoft Excel or in delimited text formats shall be produced with all underlying data un-redacted and all underlying formulas and algorithms intact.

3. Scanned Collections

a. Images files – Image files shall be Group IV TIFF files (single page files). File names cannot contain embedded spaces. The number of files per folder should be limited to 5000 files.

b. Delimited Text File – This file shall contain the IMAGEID field (image key used to reference images in Opticon). The image key shall be unique, fixed length, and the same as the Bates First number of the document. The delimited text file shall include a header record. The delimiters shall be as follows:

i) Comma – ASCII character 20
ii) Quote – ASCII character 254
iii) Newline – ASCII character 174

c. Optical Character Recognition ("OCR") text – The OCR text provided to the FTC shall be delivered as a multi-page .TXT file. The name of the file shall match the IMAGEID field. Page markers shall be placed at the beginning of each OCR text page.

d. Opticon Cross-Reference File – The Opticon cross-reference file is a comma delimited file consisting of six fields per line. There shall be a cross-reference file for every image in the database. The format for the file is as follows: ImageID, VolumeLabel, ImageFilePath, DocumentBreak, FolderBreak, BoxBreak, PageCount.

i) ImageID: The unique designation that Concordance and Opticon use to identity an image.
ii) VolumeLabel: CD/DVD volume of image/OCR TXT files.
iii) ImageFilePath: The full path to the image file.
iv) DocumentBreak: If this field contains the letter "Y", then this is the first page of a document. If this field is blank, then this page is not the first page of a document.
v) Folderbreak: Leave Blank.
vi) Boxbreak: Leave Blank
vii) PageCount: Defines the number of pages for each document.

4. Email Collections – Delimited Text with Images and Native Attachments

a. The delimited text file shall include a header record. The delimiters for the file shall be as follows:

i) Comma – ASCII character 20
ii) Quote – ASCII character 25
iii) Newline – ASCII character 174

b. The producing party shall provide a TIFF image of the email and the attachment(s), and a copy of the native attachment file(s). The text and metadata of the email and the attachment(s) shall be extracted and entered in the appropriate fields and provided as an ASCII delimited text file. All images shall be bates numbered. The email image will be the "*parent*" and the attachment(s) will be the "*child.*" An email may have more than one *child.* The *child* attachment's bates number will be listed in the *parent* email's coded fields under *CHILD_BATES.* If there is more than one attachment, list the first bates number of each attachment and separate them by semi-colons (;). The *parent* email's bates number will be listed in the *child(s)* attachment(s) under *PARENT_BATES.* The *child/children* will immediately follow the parent record. Below is a field definition table of the data requested, including hypothetical sample data:

Field	**Sample Data**	**Comment**
BEGDOC	PCC-00000001	First bates number of email
ENDDOC	PCC-00000008	Last bates number of email
BEGATTACH	PCC-00000009	First bates number of attachment(s)
ENDATTACH	PCC-00000015	Last bates number of attachment(s)
PARENT_BATES	PCC-00000001	First bates number of parent email
ATTACH_BATES	PCC-00000009, PCC-00000012	First bates number of "child" attachment(s); can be more than one bates number listed; depends on number of attachments
CUSTODIAN	Jason Wahl	Mailbox where the email resided
FROM	Jason Wahl	For email

TO	Jackie Hoel	For email
CC	Fred Thompson	For email
BCC	John McArthur	For email
EMAIL_SUBJECT	North Point Project Summary	Subject of the email
DATE_SENT	11/12/2008	Date the email was sent
TIME_SENT	04:05 PM	Time the email was sent
NATIVEFILE_LINK	D:\FTC_Production04122009 Meeting Summary\PCC-00000001.pdf	Hyperlink to native attachment (listed as file name)
DOC_EXT	.MSG, .EML, .HTML, etc.	The file extension will vary depending on whether the document is a parent email or a child attachment
AUTHOR	Jason Wahl	Attachment metadata
DATE_CREATED	11/01/2008	Attachment metadata
DATE_MOD	11/21/2008	Attachment metadata
FILE_SIZE	437,671	Attachment metadata (in KB)
PATH	K:\MGMT\SHARED\Wahl_Jason	Path where attachment file was stored
INTFILEPATH	Personal Folders/Sent Items	Location of email

TEXT	From: Wahl, Jason [PCC Corp] Sent: Tuesday, November 11, 2008 4:05 PM To: Hoel, Jackie [ABC Corp] Subject: North Point Project Summary Janice: Attached are copies of the North Point Project Summary as well as the site plan. Please let me know if you have any questions. Jason Wahl Team Lead PCC Corp 202-555-1212 - office Wahl.jason@pcccorp.com	Text of the email or attachment

5. Native Files – Native files shall be delivered with an ASCII delimited file containing the metadata associated with the files, text extracted from the native file, and a directory path to the native file. The fields to be included in the production are as follows:

FIELD	SAMPLE DATA	COMMENT
BATESFIRST	PCC-00000001	Unique sequential number
LINK	D:\SEC Production\10_01_02 Meeting Minutes\PCC-00000001.pdf	Hyperlink to native file (listed as file name)
AUTHOR	Jason Wahl	
DATE_CREATED	10/08/2009	
DATE_MOD	10/09/2009	
FILE_SIZE	765,952	
PATH	K:\MGMT\SHARED\Wahl_Jason	Path where native file was stored
CUSTODIAN	Name of the file custodian	
MD5 or SHA1	Hash Value	

Subject	Title of Document	
TEXT	Meeting Minutes for Teleconference 10/1/03 Discussion over employee stock options transpired. Decision was made to offer the options as part of the employee's Christmas bonus. Announcement was made regarding Roland Moore being promoted to Assistant Director.	Text extracted from native file

6. Media Format

a. Data may be delivered on CD, DVD, or hard drive. The media shall be encrypted. The FTC prefers to receive productions on the smallest number of media.

b. Specifications

i) Root of CD/DVD/Hard drive – two folders named Data and Images – the load files should go in the data folder and the images should go in the images folder with no more than 1000 images per folder. If you need more than one folder, please label the sub folders Vol001, Vol002, etc.

ii) CD Label shall indicate the following:

(a) Case Name
(b) Case Number
(c) Box Number
(d) Custodian Information
(e) Associated Bates Number or System Number
(f) Box(es) Source(s)
(g) CD volume

iii) Submit electronic files and images as follows:

(a) For productions over 10 gigabytes, use IDE or EIDE hard disk drives, formatted in Microsoft Windows-compatible, uncompressed data in USB 2.0 external enclosure; data shall be encrypted.

(b) For productions less than 10 gigabytes, CD-R, CD-ROM, and DVD-ROM for Windows-compatible personal computers and USB 2.0 Flash Drives are also acceptable storage formats.

iv) All documents produced in electronic format shall be scanned for and free of viruses. The FTC will return any infected media for replacement, which may affect the timing of the Company's compliance with this request.

N. **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 ways to protect such information during production. 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.

O. **Information Identification:** Each specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specifications or subspecifications to which it is responsive.

P. **Submission of Documents in lieu of Interrogatory Answers:** Previously existing documents that contain the information requested in any written Interrogatory may be submitted as an answer to the Interrogatory. In lieu of identifying documents as requested in any Interrogatory, you may, at your option, submit true copies of the documents responsive to the Interrogatory, provided that you clearly indicate the specific Interrogatory to which such documents are responsive.

Q. **Certification of Records of Regularly Conducted Activity:** Attached is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena the Company to testify at future proceedings in order to establish the admissibility of documents produced in response to this CID. You are asked to execute this Certification and provide it with your response.

SPECIFICATIONS

I. INTERROGATORIES

1. Identify the specific goal(s) or objective(s) of each security practice (and material change thereto over the applicable time period) used to prevent unauthorized access to personal information. Without limiting the response to the following example, a security practice could be to update and patch computer networks, devices, and applications, with the goal of successfully updating and patching a certain minimum number of computer networks, devices, and applications within a designated time period after updates or patches

become available (collectively, "patching procedure").

2. Identify all Hannaford employees, consultants, contractors, third-party providers, vendors, and other persons or entities with responsibility for information security (collectively, "responsible person"), describing in detail their qualifications and their roles and responsibilities as to each security practice and goal identified in response to Interrogatory Specification 1, and setting forth specifically:

   (a) the period of time during which each responsible person performed his or her roles or responsibilities as to each security practice;

   (b) the means by which Hannaford evaluated each responsible person's performance;

   (c) whether Hannaford disciplined, sanctioned, or imposed other adverse actions on any responsible person for reasons related in any way to the breach, identifying the responsible person sanctioned and the reasons for the adverse action; and

   (d) the extent to which responsive documents from the custodial files of responsible persons identified in response to Interrogatory Specification 2 have not been produced and the reasons such documents have not been produced.

3. For each security practice and goal identified in response to Interrogatory Specification 1, identify and describe in detail:

   (a) the means used to implement the security practice, the person or entity who decided on the means to be used, and the responsible person who implemented it. For example, the IT operations team could decide to use an automated patching tool to implement the patching procedure and direct a third-party provider to implement the tool;

   (b) the means used to determine the extent to which the security practice's goal or objective has been achieved (collectively, "validation process"), the person or entity responsible for conducting the validation process, and the schedule for the validation process. For example, if the patching procedure uses an automated tool implemented by a third-party provider, the validation process could involve having an employee review reports generated by the tool each week and inspect a set of applications to verify that the tool is working correctly and the reports are accurate; and

   (c) all results of validation processes.

4. Identify and describe in detail the reporting structure or hierarchy for responsible persons identified in the response to Interrogatory Specification 2, including the roles of management personnel and those who report to them.

5. Separately for Hannaford, Sweetbay, and Shop 'n Save, identify the extent of the use since 2005 of the default system administrator password ("default password") on SQL servers and applications (collectively, "SQL server") on computer networks used by each entity. The response should include, but not be limited to: (a) the name and location of SQL servers where the default password was used; how each server was used (such as to process payment card transactions or store pharmacy information); why and how frequently the default password was used; (b) why the default password was not changed after each server was installed, such as to prevent a loss of functionality that would occur if the default password were changed, and Hannaford's efforts to change the server or application so that using the default password would be unnecessary; and (c) other security measures used in lieu of changing the default password on each server.

6. Separately for Hannaford, Sweetbay, and Shop 'n Save, identify and explain in detail any material differences between the security practices used on each entity's POS networks to prevent unauthorized access to: (a) payment card information; (b) pharmacy information; and (c) personal information about employees.

7. Identify and describe in detail each marketing or promotional activity (collectively, "promotion") you undertook in response to the breach, such as providing discount coupons, gift cards, or other benefits to customers, identifying for each such promotion: the target group (such as customers who expressed concern about the breach, customers whose payment cards were or may have been exposed through the breach, or other customers and employees or prospective employees); the purpose of the promotion; the cost of the promotion; the number of customers or employees who received the promotion; and any assessment of the promotion's effectiveness in achieving its purpose.

8. Identify and describe in detail whether, and, if so, how and over what time period, customers of Hannaford, Sweetbay, or Shop 'n Save changed their purchasing practices after the breach was announced, including, but not limited to, changes in: (a) the form of payment used (such as switching from payment cards to cash and checks); (b) the average dollar amount of purchases by payment form; and (c) the churn rate or attrition rate in the customer base, reflecting the proportion of customers who stopped doing business with Hannaford, Sweetbay, and Shop 'n Save.

The response should include, but not be limited to: a separate spreadsheet for Hannaford, Sweetbay, and Shop 'n Save that sets out, week-by-week between March 17, 2007 and March 17, 2009, changes in the form of payment and average dollar amount of purchases (by individual form of payment) and the churn rate (by demographic characteristics and location); the raw data upon which each spreadsheet is based; and a detailed description of the methods used to prepare each spreadsheet.

9. To the extent not already identified in the response to Interrogatory Specification 7, identify the impact of the breach on Hannaford's sales revenue and costs, including, but not limited to, the actual cost incurred for each change made to improve information security and for consideration provided to Hannaford customers affected by the breach,

plaintiffs and potential plaintiffs, Sweetbay, Shop 'n Save, card associations, banks, credit unions, or other financial institutions.

10. Separately for Hannaford, Sweetbay, and Shop n' Save, identify on a monthly basis (or if not recorded monthly then as periodically recorded) the number and dollar value of purchases by customers by the individual form of payment (such as personal checks or cash).

11. Identify how, why, where, and by whom HAN 9641 (produced on August 27, 2008) was created, and the types and sources of personal information contained therein.

12. Identify and describe in detail the pharmacy information that is created, processed, and stored when Hannaford receives, processes, or fills a drug prescription in its pharmacies. The response should include, but not be limited to:

    (a) the types of pharmacy information that Hannaford creates, processes, or stores, such as customer name, prescription medication(s), and insurance policy number;

    (b) the pharmacy or other computer networks (such as POS networks) where each type of pharmacy information is created, processed, or stored, and the format in which it was processed or stored (such as in clear text or an encrypted format);

    (c) the period of time Hannaford retains pharmacy information;

    (d) the average weekly volume of pharmacy information that Hannaford creates, processes, or stores, including the number of unique customers the information concerns; and

    (e) the volume of pharmacy information that Hannaford created, processed, or stored while the breach was ongoing, including the number of unique customers the information concerns.

13. With respect to Hannaford's Electronic Transaction Security Policy ("Policy Statement"), which appeared on Hannaford's website and which Hannaford produced at HAN-000001 through HAN-000006, identify when the Policy Statement was made, how the Policy Statement was distributed, any modifications Hannaford made to the Policy Statement, the number of consumers who viewed the Policy Statement or the Privacy and Information Security Notice in which the Policy Statement was contained, and when the Policy Statement was withdrawn.

14. Do you contend that Hannaford was not the common point of purchase for payment cards that First Data advised Hannaford on February 27, 2008 had been subject to unauthorized account activity? If so, describe all facts, including fraud correlation information and analyses, identify all witnesses, and identify all documents on which you base your

contention. If your response is anything other than an unqualified yes, describe all facts, including the number of payment cards and the amount of fraudulent purchases made on them, identify all witnesses, and identify all documents on which you base the qualification.

15. Do you contend that no payment card or other personal information of customers was taken through the breach from: (a) Hannaford, (b) Sweetbay, and (c) Shop 'n Save? If so, for each entity describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response for each entity is anything other than an unqualified yes, describe all facts, identify all witnesses, and identify all documents on which you base the qualification.

16. Do you contend that Hannaford implemented a systematic data classification and inventory process to identify, track, and protect physical or electronic data files containing personal information? If so, describe all facts (including when the process was first implemented and all material changes thereto), identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts (including the types of personal information not subject to the process), identify all witnesses, and identify all documents on which you base the qualification.

17. Do you contend that computers on in-store POS networks could not at any time connect directly to the internet? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts (including the purposes for which the connection is used), identify all witnesses, and identify all documents on which you base the qualification.

18. Do you contend that the intruder could not have accessed administrative level accounts in the same domain in which the POS servers were members? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts, identify all witnesses, and identify all documents on which you base the qualification.

19. Do you contend that the intruder did not access administrative level accounts in the same domain in which the POS servers were members? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts, identify all witnesses, and identify all documents on which you base the qualification.

20. Do you contend that by using the BigFix patch-management product, Hannaford discharged any obligation to use readily available measures to prevent unauthorized access to personal information on computer networks? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts, identify all

witnesses, and identify all documents on which you base the qualification.

21. Do you contend that VeriSign's April 21, 2008 PCI Incident Response Report or April 29, 2008 Level 1 - PCI Data Security Standards GAP Analysis Report is inaccurate or incorrect in any material respect? If so, identify each respect in which you contend the report(s) are inaccurate or incorrect, and describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, identify each respect in which the report(s) are accurate or correct, and describe all facts, identify all witnesses, and identify all documents on which you base the qualification.

22. Do you contend that no personal information about employees (such as Social Security numbers) was processed or stored on any computer, server, or device on a Hannaford, Sweetbay, or Shop 'n Save POS network at any time during the breach? If so, for each entity describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response for each entity is anything other than an unqualified yes, describe all facts (including the names and locations of computers, servers, or devices processing or storing such information, the types and amounts of information processed or stored on the computers, servers, or devices, and whether the information was processed or stored in clear text or an encrypted format), identify all witnesses, and identify all documents on which you base the qualification.

23. Do you contend that no personal information relating to pharmacy transactions was processed or stored on any computer, server, or device on a Hannaford, Sweetbay, or Shop 'n Save POS network at any time during the breach? If so, for each entity describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response for each entity is anything other than an unqualified yes, describe all facts (including the names and locations of computers, servers, or devices processing or storing such information, the types and amounts of information processed or stored on the computers, servers, and devices, and whether the information was processed or stored in clear text or an encrypted or proprietary format), identify all witnesses, and identify all documents on which you base the qualification.

24. Setting aside compensating controls that could bring an entity into compliance with a PCI DSS requirement that otherwise would not be satisfied, do you contend that no Hannaford employee had actual knowledge that Hannaford had not fully satisfied each requirement and subpart of the PCI DSS prior to and while the breach was ongoing? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts (including each requirement and subpart that Hannaford employees had actual knowledge was not fully satisfied, the extent to which the requirement or subpart was not fully satisfied, and the mechanisms or compensating controls put in place to address the requirement or subpart not fully satisfied), identify all witnesses (including each employee with knowledge), and identify all documents on which you base the qualification.

25. Identify the custodians, sources, and physical locations of all information responsive to all Specifications of this CID, describing in detail the tools and methodologies you used to identify and locate responsive information.

II. DOCUMENTS

1. Provide all documents prepared by, or transmitted by Hannaford to, VeriSign, CyberTrust, Verizon Business, General Dynamics, IBM, Cisco, Microsoft, PricewaterhouseCoopers, or Symantec that identify, describe, investigate, evaluate, or assess Hannaford's security practices to prevent unauthorized access to personal information.

2. Provide documents sufficient to identify the time line followed in implementing critical (or equivalent) updates and patches on Hannaford, Sweetbay, and Shop 'n Save computer networks, computers, servers, devices, and applications, including, for each entity, when an update or patch became available, when it was implemented, and the extent of its implementation across networks, computers, servers, devices, and applications.

3. Separately for Hannaford, Sweetbay, and Shop 'n Save, provide all documents that relate to the use of the system administrator password, including the default password, since 2005 on SQL servers and applications (collectively, "SQL server") on computer networks used by each entity. The response should include, but not limited to:

   (a) all communications with CyberTrust regarding system administrator passwords used on servers identified in the response to Interrogatory Specification 5, including other security measures used in lieu of changing the default password;

   (b) all communications with vendors and service providers about any loss of functionality resulting from changing the default password, including requests to modify the server or applications to prevent the functionality loss; and

   (c) all communications within Hannaford or between Hannaford and any other person or entity (such as acquiring banks or the Payment Card Industry Data Security Council) regarding the use of system administrator passwords on servers identified in the response to Interrogatory Specification 3, including the consequences of using the default system administrator password.

4. Provide all documents and materials provided by or for Hannaford to VeriSign in an effort to persuade VeriSign to make changes in findings related to its: April 21, 2008 PCI Incident Response Report; or its April 29, 2008 Level 1 - PCI Data Security Standards GAP Analysis Report.

5. For the period March 17, 2007 through March 17, 2009, provide all documents that describe, evaluate, or analyze the purchasing practices of Hannaford's customers, including, but not limited to, documents that concern changes in the form of payment, the

average dollar amount of purchases (by individual form of payment), and the churn rate (by demographic characteristics and location); and the underlying data, analytical methodology, and conclusions.

6. With respect to Hannaford's Electronic Transaction Security Policy ("Policy Statement"), which appeared on Hannaford's website and which Hannaford produced at HAN-000001 through HAN-000006, provide documents sufficient to identify when the Policy Statement was made, how the Policy Statement was distributed, any modifications Hannaford made to the Policy Statement, the number of consumers who viewed the Policy Statement or the Privacy and Information Security Notice in which the Policy Statement was contained, and when the Policy Statement was withdrawn.

7. Provide all communications to or from actual or prospective acquiring banks regarding payment card transaction fees (such as interchange and discount fees), including, but not limited to: marketing materials, documents describing individual components that make up payment card transaction fees, such as security or PCI compliance; and Hannaford's contracts with acquiring banks.

8. Without redacting personal information, provide a copy of a file that is representative of the types and format of pharmacy information that is stored on computers, servers, or other devices on Hannaford and Sweetbay POS networks.

9. Provide all documents on which you base your responses to Interrogatory Specifications 14 through 24.

10. Provide the documents on which you base the responses to all the foregoing Interrogatories.

CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY

Pursuant to 28 U.S.C. § 1746

1. I, ________________________, have personal knowledge of the facts set forth below and am competent to testify as follows:

2. I have authority to certify the authenticity and accuracy of the records produced by Hannaford Bros. Co. and attached hereto.

3. The documents produced and attached hereto by Hannaford Bros. Co. are originals or true copies of records of regularly conducted activity that:

    a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

    b) Were kept in the course of the regularly conducted activity of Hannaford Bros. Co.; and

    c) Were made by the regularly conducted activity as a regular practice of Hannaford Bros. Co.

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

Executed on ____________________, 2010.

____

Signature

United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Hannaford Brothers Co.
145 Pleasant Hill Road
Scarborough, Maine 04074
Attn: Ronald C. Hodge, CEO

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

☐ You are required to appear and testify.

LOCATION OF HEARING	YOUR APPEARANCE WILL BE BEFORE
	DATE AND TIME OF HEARING OR DEPOSITION

☒ You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

☒ You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

NOV 3 0 2010

3. SUBJECT OF INVESTIGATION

See attached resolutions

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN Alain Sheer/Loretta Garrison Bureau of Consumer Protection Federal Trade Commission 601 New Jersey Avenue, NW Washington D.C. 20580	5. COMMISSION COUNSEL Alain Sheer, Bureau of Consumer Protection Federal Trade Commission 601 New Jersey Avenue, NW Washington D.C. 20580 202.326.3321
DATE ISSUED 11/2/10	COMMISSIONER'S SIGNATURE

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's *Rules of Practice* is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's *Rules of Practice* require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS:	Jon Leibowitz, Chairman Pamela Jones Harbour William E. Kovacic J. Thomas Rosch

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN A NON-PUBLIC INVESTIGATION OF UNNAMED PERSONS, PARTNERSHIPS, CORPORATIONS, OR OTHERS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF TITLE V OF THE GRAMM-LEACH-BLILEY ACT AND/OR SECTION 5 OF THE FTC ACT

File No. 002 3284

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others have engaged in or are engaging in acts or practices in violation of Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827 and/or Section 5 of the FTC Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory process available to it be used in connection with this investigation for a period not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five (5) year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five (5) year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five (5) year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; and FTC Procedures and Rules of Practice, 16 C.F.R. § 1.1 *et seq.*, and supplements thereto.

By direction of the Commission.

Donald S. Clark

Donald S. Clark
Secretary

Issued: July 16, 2009

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS:

Robert Pitofsky, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION INTO THE ACTS AND PRACTICES OF UNNAMED PERSONS, PARTNERSHIPS AND CORPORATIONS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF 15 U.S.C. § 1681 ET SEQ. AND/OR 15 U.S.C. § 45

File No. 992-3120

Nature and Scope of Investigation:

An investigation to determine whether persons, partnerships or corporations may be engaging in, or may have engaged in, acts or practices in violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and/or Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended, relating to information furnished to consumer reporting agencies, maintained in the files of consumer reporting agencies, or obtained as a consumer report from a consumer reporting agency. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. § § 46, 49, 50 and 57b-1, as amended; FTC Procedures and Rules of Practices 16 C.F.R. 1.1 et seq. and supplements thereto.

Title VI of the Consumer Credit Protection Act, Section 621, 15 USCA § 1681s.

By direction of the Commission.

Donald S. Clark

Donald S. Clark
Secretary

Dated: April 15, 1999

SECOND CIVIL INVESTIGATIVE DEMAND
TO HANNAFORD BROTHERS CO.

DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

A. **"Acquiring bank"** shall mean a bank or financial institution that provides accounts to merchants that are used in processing and settling payment card transactions for merchants.

B. **"And,"** as well as **"or,"** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in the Schedule all information that otherwise might be construed to be outside the scope of the specification.

C. **"Any"** shall be construed to include **"all,"** and **"all"** shall be construed to include the word **"any."**

D. **"The breach"** shall mean the unauthorized connection to and installation of hacker tools on Hannaford, Sweetbay, or Shop 'n Save computer networks, regarding which Hannaford was alerted on February 27, 2008 and which it disclosed publicly on March 17, 2008.

E. **"Card Association"** shall mean Visa, MasterCard, Discover, American Express, or an organization that licenses payment cards.

F. **"CID"** shall mean this Civil Investigative Demand, the attached Resolution, and the accompanying Schedule, including the Definitions, Instructions, and Specifications.

G. **"Document"** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book or label. "Document" shall also include Electronically Stored Information.

H. **"Electronically Stored Information" or "ESI"** shall mean the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created or stored information, including but not limited to electronic mail, instant messaging, videoconferencing, and direct connections or other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, cell phones, Blackberry, PDA, or other storage media, and such technical assistance or instructions as will transform such ESI into a reasonably usable form.

I. **"Each"** shall be construed to include **"every,"** and **"every"** shall be construed to include **"each."**

J. **"FTC"** or **"Commission"** shall mean the Federal Trade Commission.

K. **"Hannaford"** or the **"Company"** shall mean Hannaford Bros. Co., its parents, subsidiaries, divisions, affiliates, branches, joint ventures, and agents.

L. **"Identify"** or **"the identity of"** 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.

M. **"Payment cards"** shall mean credit cards, debit cards, electronic benefit transfer cards, gift cards, stored-value cards, insurance cards, or any other cards presented by a consumer to purchase goods or services or obtain cash.

N. **"Personal Information"** shall mean individually identifiable information from or about an individual customer including, but not limited to: (a) a first and last or business name; (b) a home, business, or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual customer's email address; (d) a telephone number; (e) a Social Security number; (f) a driver's license or other personal identification number; (g) checking account information; (h) credit, debit, EBT, bonus, loyalty, stored value, and or check-cashing card information, including card number, expiration date, security number (such as card verification value), and information stored on the magnetic stripe of the card; (i) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual customer; or (j) any information from or about an individual customer that is combined with any of (a) through (i) above.

O. **"Referring to"** or **"relating to"** shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

P. **"Shop 'n Save"** shall mean the independently owned food retailers in Maine, New Hampshire, and New York to which Hannaford sells groceries at wholesale and to which it provides payment transaction processing.

Q. **"Sweetbay"** shall mean Hannaford's sister company, Sweetbay Supermarket, which operates retail food stores in Florida.

R. **"You"** and **"Your"** shall mean the entity to which this CID is issued and includes Hannaford.

INSTRUCTIONS

A. **Certification in Lieu of Responses:** In lieu of responding to this CID, the Company may instead produce:

(1) A Certificate of Compliance, executed under oath, that its responses to the FTC's access letters of March 21, 2008, July 23, 2008, September 8, 2009, and October 14, 2009 constitute all information and non-privileged documents through December 23, 2009 that are responsive to each Specification of this CID; and

(2) A schedule of items withheld from the Company's prior productions, as required by Instruction E of this CID.

B. **Sharing of Information:** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11(c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

C. **Meet and Confer:** You must contact Alain Sheer at (202) 326-3221 as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your production of documents and information.

D. **Applicable time period:** Unless otherwise directed in the specifications, the applicable time period for the CID shall be from **January 1, 2007 until the date of full and complete compliance with this CID**. These specifications shall be deemed continuing in nature so as to require production of all documents responsive to any specification included in this CID that you have created, received, or discovered until forty-five days prior to the date of the Company's full compliance with this CID.

E. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;

2. the names, addresses, positions, and organizations of all authors and recipients of the item; and

3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

F. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. *See* 15 U.S.C. § 50; *see also* 18 U.S.C. §§ 1505, 1519. If, for any specification, there are documents that would be responsive to this CID, but they were destroyed, mislaid, transferred, deleted, altered, or over-written, describe the date and the circumstances.

G. **Petitions to Limit or Quash:** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

H. **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 Alain Sheer at (202) 326-3321. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or Assistant Regional Director. 16 C.F.R. § 2.7(c).

I. **Certification:** A responsible corporate officer shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

J. **Scope of Search:** This CID covers documents and information in your possession or under your actual or constructive custody or control including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, consultants, contractors, third-party providers, vendors, directors, officers, employees, and other agents, whether or not such documents were received from or disseminated to any person or entity.

K. **Document Production:** You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Alain Sheer, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Mail Stop NJ-8100, Washington, D.C. 20580. 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. Notice of your intended method of production shall be given by mail or telephone to Alain Sheer at (202) 326-3321 at least five days prior to the return date.

L. **Document Identification:** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. Documents should be produced in the order in which they appear in your files and without being shuffled or otherwise rearranged; if documents are removed from their original folders, binders, covers, or containers in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, or container from which such documents came. In addition, number by page all documents in your submission and indicate the total number of documents in your submission. Also number all media in your submission which contain ESI and indicate the contents of the media. For media containing ESI, identify the file path where each of the individual files is located.

M. **Production of Copies:** Unless otherwise stated, legible photocopies may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of original documents may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request. 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.

N. **Submission of Electronic Data:** The following guidelines refer to any documents that you choose to provide in electronic form. You must confirm with the FTC that the proposed electronic data formats and media types will be acceptable to the government.

1. Magnetic and other electronic media types accepted

   (a) CD-R CD-ROMs formatted to ISO 9660 specifications.

   (b) DVD-ROM for Windows-compatible personal computers.

   (c) IDE and EIDE hard disk drives up to 300GB per drive, formatted in Microsoft Windows-compatible, uncompressed data.

   Note: Other types of tape media used for archival, backup or other purposes such as 4mm & 8mm DAT and other cassette, mini-cartridge, cartridge, and DAT/helical scan tapes, DLT or other types of media **accepted only with prior**

approval.

2. File and record formats

(a) E-mail: The FTC accepts MS Outlook PST files, MS Outlook MSG files. Any other electronic submission of email accepted only with prior approval.

(b) Scanned Documents: Image submissions accepted with the understanding that unreadable images will be resubmitted in original, hard copy format in a timely manner. Scanned documents must adhere to the following specifications:

(i) All images must be multi-page, 300 DPI - Group IV TIFF files named for the beginning bates number.

(ii) If the full text of the document is available, that should be provided as well. The text should be provided in one file for the entire document or email, named the same as the first TIFF file of the document with a *.TXT extension.

Note: Single-page, 300 DPI – Group IV TIFF files may be submitted **with prior approval** if accompanied by an acceptable load file such as a Summation or Concordance image load file which denotes the appropriate information to allow the loading of the images into a document management system with all document breaks (document delimitation) preserved. OCR accompanying single-page TIFF submissions should be located in the same folder and named the same as the corresponding TIFF page it was extracted from, with a *.TXT extension.

(c) Other PC files: The FTC accepts word processing documents in ASCII text, WordPerfect version 10 or earlier, or Microsoft Word 2002 version or earlier. Spreadsheets should be in MS Excel 2002 (*.xls) version or earlier. Database files should be in MS Access 2002 or earlier. PowerPoint presentations may be submitted in MS PowerPoint 2002 or earlier. Other proprietary formats for PC files should not be submitted without prior approval. Files may be submitted using the compressed ZIP format to reduce size and ease portability. Adobe Acrobat PDF (*.pdf) may be submitted where the normal business practice storage method is PDF.

Note: Database files may also be submitted **with prior approval** as delimited ASCII text files, with field names as the first record, or as fixed-length flat files with appropriate record layout. For ASCII text files, field-level documentation should also be provided and care taken so that delimiters and quote characters do not appear in the data. The FTC may require a sample of the data to be sent for testing.

3. Security

(a) All submissions of electronic data to the FTC must be free of computer viruses. In addition, any passwords protecting documents or files must be removed or provided to the FTC.

(b) Magnetic media shall be carefully packed to avoid damage and must be clearly marked on the outside of the shipping container: "MAGNETIC MEDIA – DO NOT X-RAY, MAY BE OPENED FOR POSTAL INSPECTION."

O. **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 ways to protect such information during production. 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 <u>in combination with</u> 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.

P. **Information Identification:** Each specification and sub-specification of this CID shall be answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specifications or subspecifications to which it is responsive.

Q. **Submission of Documents in lieu of Interrogatory Answers:** Previously existing documents that contain the information requested in any written Interrogatory may be submitted as an answer to the Interrogatory. In lieu of identifying documents as requested in any Interrogatory, you may, at your option, submit true copies of the documents responsive to the Interrogatory, provided that you clearly indicate the specific Interrogatory to which such documents are responsive.

R. **Certification of Records of Regularly Conducted Activity:** Attached is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena the Company to testify at future proceedings in order to establish the admissibility of documents produced in response to this CID. You are asked to execute this Certification and provide it with your response.

<u>SPECIFICATIONS</u>

I. INTERROGATORIES

1. Identify the complete legal name of Hannaford and all other names under which it has done or does business, its corporate mailing address, and the date and state of

incorporation.

2. Identify and describe Hannaford's parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, websites, entities over which it exercises supervision or control, entities for which it provides services (such as processing credit and debit card transactions), and independently-owned entities that sell Hannaford products. For each such entity, describe in detail the nature of its relationship to Hannaford, and, where applicable, describe in detail the services and identify the types of products that Hannaford provides.

3. Identify the name, location, and operating system of each computer network ("network") Hannaford used to store, maintain, process, transmit, handle, or otherwise use (collectively hereinafter, "store and process") personal information (such as to prepare, send, and receive authorization requests for credit and debit card transactions) for itself and other entities prior to the breach.

4. For each network identified in the response to Interrogatory Specification 3, above, for the period beginning on **January 1, 2005**:

   (a) identify the types of personal information stored and processed on the network, the source of each type of information (including, but not limited to: credit, debit, EBT, or stored value cards; information provided by customers to obtain discount coupons or check cashing, bonus, or loyalty cards, whether online, over the telephone, or in person; and information provided by Sweetbay Supermarkets, independently-owned entities selling Hannaford products, and other third parties), and describe in detail how each type of information is stored and processed by Hannaford;

   (b) provide a narrative that describes in detail the components of the network, explains the functions of the components, and describes how the components operate together on the network;

   (c) provide the names, titles, and contact information of the individuals responsible for creating, designing, managing, securing, and updating the network; and

   The responses to this Interrogatory should describe in detail each material change or update to each network that has been made that concerns, refers, or relates to the subpart, as well as the date the change or update was implemented and the reasons for the change or update.

5. Describe in detail the 2007 upgrades Hannaford made to its wireless encryption, including the encryption practices in place before and after the upgrade, and the devices involved in the upgrade (*e.g.*, POS terminals or wireless access points), and identifying the stores or other locations where the upgrades were implemented.

6. Describe how and when Hannaford first learned about the breach.

7. Identify how (such as by public announcement or individual breach notification letter), when, how many, and by whom customers were notified that their information was or may have been obtained without authorization. Explain why customers were notified, and provide a copy of each substantively different notification. If notification was not provided as soon as Hannaford became aware of the breach or was not provided to all affected customers or at all, explain why not.

8. Identify and describe in detail the security measures Hannaford has implemented to address the breach, including, but not limited to, efforts to protect personal information stored or processed on its computer networks.

9. Describe the nature of the breach as it relates to pharmacy information, setting forth specifically:

   (a) the name, location, and operating system of each computer network Hannaford used to store and process information related to pharmacy transactions, pharmacy customer files, and "protected health information," as that term is defined in 45 CFR § 160.103 (collectively, "pharmacy information"), including, but not limited to, networks located within pharmacies in Hannaford stores, other networks in the stores, and networks located at Hannaford's headquarters, datacenter, and distribution centers (collectively, "pharmacy networks");

   (b) the types of pharmacy information stored and processed on each pharmacy network and the source of each type of information;

   (c) a narrative that describes in detail the components of the network, explains the functions of the components, and describes how the components operate together on the network;

   (d) the security procedures, practices, policies, and defenses (such as access controls or encryption) used to protect pharmacy information from unauthorized access while stored, processed, or transmitted within a network or between networks; and

   (e) the complete legal name of each entity that owns, operates, or otherwise controls the operation of each pharmacy located in a Hannaford store, and for each such entity, describe in detail the nature of its relationship to Hannaford;

   (f) the names, titles, and contact information of the individuals responsible for creating, designing, managing, securing, and updating the pharmacy networks; and

The responses to this Interrogatory should describe in detail each material change or update to each pharmacy network that has been made that concerns, refers, or relates to the subpart, as well as the date the change or update was implemented and the reasons for the change or update.

10. Describe in detail Hannaford's maintenance of pharmacy information on the POS servers, setting forth specifically:

    (a) a narrative describing the types of pharmacy information maintained on the POS servers;

    (b) the location of the POS servers within Hannaford's networks;

    (c) the periods of time for which pharmacy information was maintained on the POS servers;

    (d) how Hannaford backs-up its pharmacy information, explaining the reasons Hannaford changed any of its back-up procedures; and

    (e) when pharmacy information maintained on the POS server was first encrypted, explaining the reasons Hannaford changed any of its encryption practices.

11. Describe in detail the processes Hannaford uses to obtain authorization for credit or debit card transactions ("card authorization") for itself and other entities. The response should:

    (a) set forth the complete transmission or flow path for authorization requests and responses and the underlying information for each network involved in any way in card authorization, starting with the collection of information from a card at a POS terminal or cash register, continuing to formatting the information into an authorization request, transmitting the authorization request to the acquiring bank, the bank association network, and the issuing bank, and ending with receiving the response to the authorization request;

    (b) identify each portion of the transmission or flow paths set out in the response to Interrogatory Specification 11(a) where authorization requests, authorization responses, or the underlying personal information were transmitted in clear text, as well as the time period during which the requests, responses and information were transmitted in clear text;

    (c) identify the computers or servers used to aggregate authorization requests from individual stores and transmit them to bank associations and banks ("card authorization server"), and, for each card authorization server, identify the applications used for card authorization and the services enabled on the server, and describe in detail how the server has been protected from unauthorized access (such as protected by its own firewall); and

(d) describe in detail how and where authorization requests and responses and underlying personal information are stored or maintained (such as by being stored on a card authorization server or written to transaction logs located elsewhere on a network), as well as how stored or maintained requests, responses, and information have been protected from unauthorized access.

12. Identify each service related to processing electronic payment transactions for Shop 'n Save and Sweetbay, including, but not limited to: authorization services through which Hannaford receives credit, debit, and EBT card authorization requests from Shop 'n Save or Sweetbay, transmits the requests through Hannaford networks to issuing banks, government agencies, or card associations, receives responses to the requests, and transmits the responses back to the Shop 'n Save or Sweetbay stores where the requests originated; check collection and processing services; automated clearinghouse processing; providing software or hardware that Shop 'n Save or Sweetbay use in conjunction with a service; providing sales data for transactions processed at Shop 'n Save or Sweetbay; providing network services; providing settlement services; or providing transaction history information.

13. For each service identified in the response to Interrogatory Specification 12:

(a) describe in detail the components and operation of the service;

(b) identify the name and address of each Shop 'n Save and Sweetbay store to which Hannaford provides the service;

(c) identify the annual revenue or cost savings (such as a volume discount on processing fees on transactions that originate at Hannaford's stores) Hannaford derives from providing each service, reporting revenue or cost saving separately for Shop 'n Save, Sweetbay, and stores operated by other entities.

14. Describe Hannaford's payment processing and related services, including, but not limited to, a narrative setting forth:

(a) separately for Shop 'n Save and Sweetbay, the number and dollar value of card transactions processed monthly (or if not recorded on a monthly basis, then as periodically recorded);

(b) for Hannaford, the number and dollar value of payment card transactions processed monthly (or if not recorded on a monthly basis, then as periodically recorded);

(c) monthly records or invoices (or if not recorded or invoiced monthly, then as periodically recorded or invoiced) of Hannaford's charges for each separate component of the services (such as POS equipment, maintenance, interchange fees, and other payment card fees);

(d) monthly records (or if not recorded monthly, then as periodically recorded) of the costs Hannaford recovered from Shop 'n Save and from Sweetbay for each component of the services; and

(e) monthly records (or if not recorded monthly, then as periodically recorded) of the interchange and other payment fees incurred by Hannaford for card transactions in Hannaford stores.

15. With respect to Hannaford's payroll check cashing program, identify:

(a) the number of payroll checks Hannaford cashes annually;

(b) the number of customers for whom Hannaford has cashed payroll checks;

(c) the nature of the relationship between Hannaford and individuals presenting payroll checks to be cashed (for example, retail customers); and

(d) the application or other process followed to enroll individuals in the check cashing program, including the information an individual must provide to enroll.

16. Describe in detail Hannaford's policies and procedures to ensure compliance with Section 615(a) of the FCRA ("Section 615(a)") as it relates to approving or declining personal checks customers present to Hannaford, Sweetbay, or Shop 'n Save to pay for their purchases or obtain cash, setting forth specifically how adverse action notices are provided to customers whose personal checks have been declined.

17. Identify the types of information that vendors, such as SCAN, provide to Hannaford for use in approving or declining personal checks presented to Hannaford, Sweetbay, and Shop 'n Save, setting forth specifically the items of information that each vendor provides and describing how Hannaford obtains access to the information (such as connecting remotely to a server on the vendor's network or by connecting directly to a server on Hannaford's network where the information is stored).

18. Separately for Hannaford, Sweetbay, and Shop 'n Save, identify:

(a) the annual total number of personal checks that were declined; and

(b) the annual total number of adverse action notices that were provided to customers whose checks were declined.

19. Identify each material factual statement or assertion in VeriSign's April 21, 2008 PCI Incident Response Report that you dispute, explaining in detail the bases for your position.

20. With respect to the PCI assessment performed by CyberTrust in January and February

2008, identify which networks and components, if any, were not included in the assessment, explaining the reasons these networks and components were not included and identifying who decided to exclude them.

21. Describe in detail the harms and injuries resulting from the breach, including, but not limited to, a narrative setting forth:

(a) the number of payment cards of all kinds that were or may have been compromised;

(b) the number of payment cards of all kinds that have been used to make fraudulent purchases, setting forth the dollar value of the fraudulent purchases;

(c) the number of cards of all kinds that have been cancelled and re-issued, setting forth the costs of doing so by type of card;

(d) the number of government identification cards (such as driver's license or Social Security cards) that have been cancelled and re-issued, and setting forth the costs of doing so by type of card; and

(e) the number of checking or other bank accounts that were closed and reopened at a different institution or under a different account number, setting forth the costs of doing so.

II. DOCUMENTS

1. Provide all documents prepared by or for Hannaford that identify, describe, investigate, evaluate, or assess: (a) how the breach occurred; (b) the time period over which it occurred; (c) where the breach began (*e.g.*, what the point of entry was and whether it was located in a store or on a central network linking stores); (d) the path the intruder followed from the point of entry to the information compromised and then in exporting or downloading the information (including all intermediate steps); and (e) the types and amounts of information that were or may have been accessed without authorization.

Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in the breach; reports of penetration and gap analysis; logs that record the intruder's steps in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was misconfigured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of the breach prepared internally and by third-parties; and other records relating or referring to the breach, including minutes or notes of meetings attended by Hannaford personnel and documents that identify the attackers.

2. Provide documents sufficient to identify applications or programs used to store, transmit, or process personal information up to the time of the breach on each computer network identified in the response to Interrogatory Specification 3, as well as documents that concern, relate, or refer to the applications or programs, including, but not limited to, contracts, operating manuals, user guides, and communications with the vendors of the applications or programs.

3. Provide all documents that concern, relate, or refer to fraud stemming from the breach and the consequences of the fraud. Responsive documents should include, but not be limited to:

   (a) fraud reports, alerts, or warnings issued by bank associations, banks, or other entities; lists identifying credit, debit, and other types of cards that have been used without authorization or may have been exposed by the breach as well as the issuing banks; documents that assess, identify, evaluate, estimate, or predict the amount of fraudulent purchases resulting from the breach; claims made against Hannaford's acquiring banks under bank network alternative dispute resolution programs (*e.g.*, pre-compliance and compliance actions), and the resolution of any such claims; claims made against Hannaford by banks that issued cards that have been used for unauthorized purchases (such as by demand letters); claims of fraud and/or identity theft, including, but not limited to, affidavits filed by consumers with their banks; and documents that assess, identify, evaluate, estimate, or predict the number of credit, debit, and other types of cards that have been cancelled and/or reissued, the cost per card and in total of cancelling and/or reissuing cards, and additional costs attributable to the breach (such as for increased monitoring for fraud or providing fraud insurance to consumers affected by the breach); and

   (b) documents relating to investigations of or complaints filed with or against Hannaford relating to the breach, including, but not limited to, private lawsuits, customer correspondence with Hannaford, and documents filed with federal, state, or local government agencies, federal or state courts, and Better Business Bureaus.

4. Provide all documents that concern, relate, or refer to Hannaford's compliance with the Payment Card Industry Data Security Standard or any other industry security requirements in its capacity as a merchant and in its capacity as a provider of card authorization services to other entities. Responsive documents should include, but not be limited to: each security assessment, audit, evaluation, investigation, study, penetration or other test, remediation, certification, and accreditation (collectively, "tests") conducted, performed, or prepared by or for Hannaford or a bank association, bank, or other entity;

documents that set out the scope of each test (such as whether some rather than all components on a network were included in the test); and documents that question, challenge, contest, warn, or complain about the adequacy of security provided by Hannaford.

5. Provide documents sufficient to identify all claims, representations, and statements made by Hannaford regarding its collection, disclosure, use, and protection of personal information, including any policies or statements relating to how Hannaford secures personal information, indicating for each policy or statement the dates when it was adopted or made, to whom it was distributed, and all means by which it was distributed.

6. Provide documents sufficient to identify any other instances (besides the breach) of unauthorized access to Hannaford's computer networks of which Hannaford is aware, as well as the types of information accessed without authorization and when the unauthorized access occurred.

7. Provide documents sufficient to set forth the complete transmission or flow path for personal information within and between computer networks used or operated by or for Hannaford, Sweetbay, and Shop 'n Save, and identify each portion of the transmission or flow path over which personal information (in any form or format) was transmitted in clear text, each point in the flow path where personal information was stored in clear text, as well as the time period during which the information was transmitted or stored in clear text.

8. Provide copies of all substantially different documents that set out the terms and conditions under which Hannaford provides services related to processing electronic payment transactions for Shop 'n Save and Sweetbay, including, but not limited to, contracts to supply the service as well as hardware, software, or technical support used in providing the service.

9. Provide documents setting out the operation of the Service Plus card program, as well as a detailed description of the program. The response should include, but not be limited to, documents and descriptions that set out: the nature and extent of the program, including whether the cards are issued in conjunction with a bank or financial institution; the program's terms and conditions, including the processes by which individuals and institutions are approved to participate in the program; the services provided by and/or benefits obtained through the program (such as advancing credit for purchases); the types and amounts of personal information from or about individuals that Hannaford stores and processes in conjunction with the program; the means by which Hannaford is paid for purchases made using Service Plus cards (such as preparing and submitting electronic checks drawn on a customer's checking account); the number of individuals that participate in the program; the total number of Service Plus cards Hannaford has issued to individuals; and the annual revenue from sales to individuals under the program.

10. With respect to the PCI assessments performed by CyberTrust in January and February

2008, provide documents sufficient to identify the scope of work for the assessment. Responsive documents should include, but not be limited to: contracts; a Statement of Work; documents identifying each network, computer, server, application, and other network component to which the PCI applies (the "PCI system"); documents explaining how CyberTrust and/or Hannaford selected the particular networks and components of the PCI system on which to conduct the assessment (the "assessment sample"); and communications in any form between Hannaford and CyberTrust that discuss, resolve, dispute, or relate to the composition of the assessment sample or findings and issues set out in preliminary and final versions of the assessment.

11. Provide a copy of each substantially different privacy notice (initial and annual) provided to customers for whom Hannaford cashed payroll checks and customers for whom Hannaford cashed personal checks.

12. Provide copies of documents settling claims and/or reimbursing claims for costs related to the breach.

13. Provide a copy of each substantially different contract with Catalina.

14. For each network identified in response to Interrogatory Specification 3, for the period beginning on January 1, 2005, provide:

(a) all blueprints and diagrams setting out in detail the components, topology, and architecture of the network. Responsive documents should include, but not be limited to, documents that identify and locate the components of the network, such as computers, POS devices, cash registers, remote access equipment (such as wireless access points), servers, firewalls, routers, internet, private line, and other connections, connections to other Hannaford networks and outside networks, and security mechanisms and devices (such as intrusion detection systems);

(b) detailed schemes, diagrams, and blueprints of the databases that contain personal information (including table and field names) and identify the computers, servers, or other devices where the databases reside;

(c) documents setting out the security procedures, practices, policies, and defenses (such as access controls or encryption) in place to protect personal information from unauthorized access while stored on the network, transmitted within the network or between networks, and/or processed on the network; and

(d) provide all documents that concern, relate, or refer to security vulnerabilities in the network, including, but not limited to, documents identifying vulnerabilities, documents setting out and explaining the measures implemented to address the vulnerabilities, and communications, such as emails, that assess, question, or describe the state of security, warn of vulnerabilities, or propose or suggest changes in security measures.

15. Provide all documents relating to whether the breach affected pharmacy information, including, but not limited to, audits or assessments.

16. For each pharmacy network identified in response to Interrogatory Specification 10, provide:

(a) blueprints and diagrams setting out in detail the components, topology, and architecture of the network. Responsive documents should include, but not be limited to, documents that identify and locate the components of the network, such as: computers; POS devices; cash registers; remote access equipment (such as wireless access points); servers; firewalls; routers; internet, private line, and other connections; connections to other Hannaford networks and outside networks; and security mechanisms and devices (such as intrusion detection systems);

(b) documents setting out the security procedures, practices, policies, and defenses (such as access controls or encryption) used to protect pharmacy information from unauthorized access while stored, processed, or transmitted within a network or between networks; and

(c) documents sufficient to set forth the complete transmission or flow path for pharmacy information between and within computer networks used or operated by or for Hannaford, and identify each portion of the transmission or flow path where pharmacy information was transmitted in clear text, each point in the flow path where pharmacy information was stored in clear text, as well as the time period during which the information was transmitted or stored in clear text; and

(d) documents that concern, relate, or refer to security vulnerabilities in pharmacy networks, including, but not limited to, documents identifying vulnerabilities, documents setting out and explaining the measures implemented to address the vulnerabilities, and communications, such as emails, that assess, question, or describe the state of security, warn of vulnerabilities, or propose or suggest changes in security measures.

17. Provide documents sufficient to identify the policies and procedures implemented to ensure compliance with Section 615(a) of the FCRA ("Section 615(a)") as it relates to approving or declining personal checks customers present to Hannaford, Sweetbay, or Shop 'n Save to pay for their purchases or obtain cash. Responsive documents should include, but not be limited to:

(a) a copy of each substantially different policy or procedure that relates to approving or declining personal checks;

(b) copies of materials and other instructions given to employees to train them about their obligations to ensure compliance with Section 615(a);

(c) documents setting forth the results of testing, monitoring, and evaluations of the extent of compliance with Section 615(a);

(d) customer complaints about compliance with Section 615(a), and investigations of the complaints;

(e) documents filed with federal, state, or local government agencies, federal or state courts, and Better Business Bureaus that relate to compliance with Section 615(a); and

(f) a copy of each substantially different adverse action notice that has been provided to customers.

18. Provide a copy of each contract with a vendor, such as SCAN, that provides information that Hannaford uses in any way to approve or decline personal checks presented at Hannaford, Sweetbay, and Shop 'n Save.

CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY
Pursuant to 28 U.S.C. § 1746

1. I, __________________________, have personal knowledge of the facts set forth below and am competent to testify as follows:

2. I have authority to certify the authenticity and accuracy of the records produced by Hannaford Bros. Co. and attached hereto.

3. The documents produced and attached hereto by Hannaford Bros. Co. are originals or true copies of records of regularly conducted activity that:

   a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

   b) Were kept in the course of the regularly conducted activity of Hannaford Bros. Co.; and

   c) Were made by the regularly conducted activity as a regular practice of Hannaford Bros. Co.

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

Executed on ____________________, 2010.

____

Signature

United States of America
Federal Trade Commission

CIVIL INVESTIGATIVE DEMAND

1. TO

Kash n' Karry Food Stores, Inc.
3801 Sugar Palm Drive
Tampa, Florida 33619

This demand is issued pursuant to Section 20 of the Federal Trade Commission Act, 15 U.S.C. § 57b-1, in the course of an investigation to determine whether there is, has been, or may be a violation of any laws administered by the Federal Trade Commission by conduct, activities or proposed action as described in Item 3.

2. ACTION REQUIRED

□ You are required to appear and testify.

LOCATION OF HEARING	YOUR APPEARANCE WILL BE BEFORE
	DATE AND TIME OF HEARING OR DEPOSITION

☒ You are required to produce all documents described in the attached schedule that are in your possession, custody, or control, and to make them available at your address indicated above for inspection and copying or reproduction at the date and time specified below.

☒ You are required to answer the interrogatories or provide the written report described on the attached schedule. Answer each interrogatory or report separately and fully in writing. Submit your answers or report to the Records Custodian named in Item 4 on or before the date specified below.

DATE AND TIME THE DOCUMENTS MUST BE AVAILABLE

3. SUBJECT OF INVESTIGATION

See attached resolutions

4. RECORDS CUSTODIAN/DEPUTY RECORDS CUSTODIAN Alain Sheer/Loretta Garrison Bureau of Consumer Protection Federal Trade Commission 601 New Jersey Avenue, NW Washington D.C. 20580	5. COMMISSION COUNSEL Alain Sheer, Bureau of Consumer Protection Federal Trade Commission 601 New Jersey Avenue, NW Washington DC 20580 202.326.3321
DATE ISSUED 12/6/10	COMMISSIONER'S SIGNATURE

INSTRUCTIONS AND NOTICES

The delivery of this demand to you by any method prescribed by the Commission's Rules of Practice is legal service and may subject you to a penalty imposed by law for failure to comply. The production of documents or the submission of answers and report in response to this demand must be made under a sworn certificate, in the form printed on the second page of this demand, by the person to whom this demand is directed or, if not a natural person, by a person or persons having knowledge of the facts and circumstances of such production or responsible for answering each interrogatory or report question. This demand does not require approval by OMB under the Paperwork Reduction Act of 1980.

PETITION TO LIMIT OR QUASH

The Commission's Rules of Practice require that any petition to limit or quash this demand be filed within 20 days after service, or, if the return date is less than 20 days after service, prior to the return date. The original and twelve copies of the petition must be filed with the Secretary of the Federal Trade Commission, and one copy should be sent to the Commission Counsel named in Item 5.

YOUR RIGHTS TO REGULATORY ENFORCEMENT FAIRNESS

The FTC has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action.

The FTC strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

TRAVEL EXPENSES

Use the enclosed travel voucher to claim compensation to which you are entitled as a witness for the Commission. The completed travel voucher and this demand should be presented to Commission Counsel for payment. If you are permanently or temporarily living somewhere other than the address on this demand and it would require excessive travel for you to appear, you must get prior approval from Commission Counsel.

Form of Certificate of Compliance*

I/We do certify that all of the documents and information required by the attached Civil Investigative Demand which are in the possession, custody, control, or knowledge of the person to whom the demand is directed have been submitted to a custodian named herein.

If a document responsive to this Civil Investigative Demand has not been submitted, the objections to its submission and the reasons for the objection have been stated.

If an interrogatory or a portion of the request has not been fully answered or a portion of the report has not been completed, the objections to such interrogatory or uncompleted portion and the reasons for the objections have been stated.

Signature ______________________________

Title ______________________________

Sworn to before me this day

____________________ ______

____
Notary Public

____

*In the event that more than one person is responsible for complying with this demand, the certificate shall identify the documents for which each certifying individual was responsible. In place of a sworn statement, the above certificate of compliance may be supported by an unsworn declaration as provided for by 28 U.S.C. § 1746.

UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION

COMMISSIONERS: Jon Leibowitz, Chairman
Pamela Jones Harbour
William E. Kovacic
J. Thomas Rosch

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN A NON-PUBLIC INVESTIGATION OF UNNAMED PERSONS, PARTNERSHIPS, CORPORATIONS, OR OTHERS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF TITLE V OF THE GRAMM-LEACH-BLILEY ACT AND/OR SECTION 5 OF THE FTC ACT

File No. 002 3284

Nature and Scope of Investigation:

To determine whether unnamed persons, partnerships, corporations, or others have engaged in or are engaging in acts or practices in violation of Title V of the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809, 6821-6827 and/or Section 5 of the FTC Act, 15 U.S.C. § 45, as amended. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory process available to it be used in connection with this investigation for a period not to exceed five (5) years from the date of issuance of this resolution. The expiration of this five (5) year period shall not limit or terminate the investigation or the legal effect of any compulsory process issued during the five (5) year period. The Federal Trade Commission specifically authorizes the filing or continuation of actions to enforce any such compulsory process after the expiration of the five (5) year period.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. §§ 46, 49, 50, and 57b-1, as amended; and FTC Procedures and Rules of Practice, 16 C.F.R. § 1.1 *et seq.*, and supplements thereto.

By direction of the Commission.

Donald S. Clark

Donald S. Clark
Secretary

Issued: July 16, 2009

UNITED STATES OF AMERICA
BEFORE FEDERAL TRADE COMMISSION

COMMISSIONERS:

Robert Pitofsky, Chairman
Sheila F. Anthony
Mozelle W. Thompson
Orson Swindle

RESOLUTION DIRECTING USE OF COMPULSORY PROCESS IN NONPUBLIC INVESTIGATION INTO THE ACTS AND PRACTICES OF UNNAMED PERSONS, PARTNERSHIPS AND CORPORATIONS ENGAGED IN ACTS OR PRACTICES IN VIOLATION OF 15 U.S.C. § 1681 ET SEQ. AND/OR 15 U.S.C. § 45

File No. 992-3120

Nature and Scope of Investigation:

An investigation to determine whether persons, partnerships or corporations may be engaging in, or may have engaged in, acts or practices in violation of the Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq., and/or Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, as amended, relating to information furnished to consumer reporting agencies, maintained in the files of consumer reporting agencies, or obtained as a consumer report from a consumer reporting agency. Such investigation shall, in addition, determine whether Commission action to obtain redress of injury to consumers or others would be in the public interest.

The Federal Trade Commission hereby resolves and directs that any and all compulsory processes available to it be used in connection with this investigation.

Authority to Conduct Investigation:

Sections 6, 9, 10, and 20 of the Federal Trade Commission Act, 15 U.S.C. § § 46, 49, 50 and 57b-1, as amended; FTC Procedures and Rules of Practices 16 C.F.R. 1.1 et seq. and supplements thereto.

Title VI of the Consumer Credit Protection Act, Section 621, 15 USCA § 1681s.

By direction of the Commission.

Donald S. Clark

Donald S. Clark
Secretary

Dated: April 15, 1999

FIRST CIVIL INVESTIGATIVE DEMAND TO KASH N' KARRY FOOD STORES, INC.

DEFINITIONS

As used in this Civil Investigative Demand, the following definitions shall apply:

A. **"Acquiring bank"** shall mean a bank or financial institution that provides accounts to merchants that are used in processing and settling payment card transactions for merchants.

B. **"And,"** as well as **"or,"** shall be construed both conjunctively and disjunctively, as necessary, in order to bring within the scope of any specification in the Schedule all information that otherwise might be construed to be outside the scope of the specification.

C. **"Any"** shall be construed to include **"all,"** and **"all"** shall be construed to include the word **"any."**

D. **"The breach"** shall mean the unauthorized connection to and installation of hacker tools on Hannaford, Sweetbay, or Shop 'n Save computer networks, regarding which Hannaford was alerted on February 27, 2008 and which it disclosed publicly on March 17, 2008.

E. **"Card Association"** shall mean Visa, MasterCard, Discover, American Express, or an organization that licenses payment cards.

F. **"CID"** shall mean this Civil Investigative Demand, the attached Resolution, and the accompanying Schedule, including the Definitions, Instructions, and Specifications.

G. **"Document"** shall mean the complete original and any non-identical copy (whether different from the original because of notations on the copy or otherwise), regardless of origin or location, of any written, typed, printed, transcribed, filmed, punched, or graphic matter of every type and description, however and by whomever prepared, produced, disseminated or made, including but not limited to any advertisement, book, pamphlet, periodical, contract, correspondence, file, invoice, memorandum, note, telegram, report, record, handwritten note, working paper, routing slip, chart, graph, paper, index, map, tabulation, manual, guide, outline, script, abstract, history, calendar, diary, agenda, minute, code book or label. "Document" shall also include Electronically Stored Information.

H. **"Electronically Stored Information" or "ESI"** shall mean the complete original and any non-identical copy (whether different from the original because of notations, different metadata, or otherwise), regardless of origin or location, of any electronically created or stored information, including but not limited to electronic mail, instant messaging, videoconferencing, and direct connections or other electronic correspondence (whether active, archived, or in a deleted items folder), word processing files, spreadsheets, databases, and sound recordings, whether stored on cards, magnetic or electronic tapes, disks, computer files, computer or other drives, cell phones, Blackberry, PDA, or other storage media, and such technical assistance or instructions as will transform such ESI into a reasonably usable form.

I. **"Each"** shall be construed to include **"every,"** and **"every"** shall be construed to include **"each."**

J. **"FTC"** or **"Commission"** shall mean the Federal Trade Commission.

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

L. **"Identify"** or **"the identity of"** 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.

M. **"Payment cards"** shall mean credit cards, debit cards, electronic benefit transfer cards, gift cards, stored-value cards, insurance cards, or any other cards presented by a consumer to purchase goods or services or obtain cash.

N. **"PCI compliance"** shall mean compliance with the Payment Card Industry Data Security Standard, which is established by the Payment Card Industry Data Security Council.

O. **"Personal Information"** shall mean individually identifiable information from or about an individual consumer including, but not limited to: (a) a first and last name; (b) a home or physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a telephone number; (e) a date of birth; (f) payment card information, including card number, expiration date, electronic security code, and data stored on the magnetic stripe of a card; (g) a Personal Identification Number for a payment card; (h) a government-issued identification number, such as a driver's license, military identification, passport, or Social Security number; (i) an employee identification number; (j) bank routing, account, and check numbers; (k) personal check cashing history; (l) pharmacy information; (m) income, employment, retirement, disability, and medical records; (n) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual consumer; and (o) any information that is combined with any of (a) through (n) above. For the purpose of this provision, a "consumer" shall include an "employee" and an individual seeking to become an employee, where "employee" shall mean an agent, servant, salesperson, associate, independent contractor, and other person directly or indirectly under the control of Sweetbay.

P. **"Pharmacy Information"** shall mean information that is created, processed, and stored when Sweetbay receives, processes, or completes a transaction in a pharmacy, including, but not limited to, "protected health information," as that term is defined in 45 CFR § 160.103, prescription information, such as medication and dosage, prescribing physician name, address, and telephone number, health insurer name, and insurance account and policy numbers; reports or files on controlled substances, pharmacy customer files, and flexible spending accounts or other similar customer accounts.

Q. **"POS networks"** shall mean computers, servers, devices, and applications located in stores that are used to: (a) process and complete consumer purchases, including, but not limited to, purchases made with payment cards, checks, and cash, and (b) provide other services, such as cashing personal and payroll checks.

R. **"Process or store"** shall mean to maintain, transmit, handle, process, store, or otherwise use in any way.

S. **"Referring to"** or **"relating to"** shall mean discussing, describing, reflecting, containing, analyzing, studying, reporting, commenting, evidencing, constituting, setting forth, considering, recommending, concerning, or pertaining to, in whole or in part.

T. **"Security practice"** shall mean security procedures, practices, policies, and defenses.

U. **"Shop 'n Save"** shall mean the independently owned food retailers in Maine, New Hampshire, and New York to which Hannaford sells groceries at wholesale and to which it provides payment transaction processing.

V. **"Sweetbay"** or the **"Company"** shall mean Kash n' Karry Food Stores, Inc. (d/b/a Sweetbay Supermarket), its wholly or partially owned subsidiaries, unincorporated divisions, joint ventures, operations under assumed names, and affiliates, and all directors, officers, employees, agents, consultants, and other persons working for or on behalf of the foregoing.

W. **"You"** and **"Your"** shall mean the entity to which this CID is issued and includes Sweetbay.

INSTRUCTIONS

A. **Sharing of Information:** The Commission often makes its files available to other civil and criminal federal, state, local, or foreign law enforcement agencies. The Commission may make information supplied by you available to such agencies where appropriate pursuant to the Federal Trade Commission Act and 16 C.F.R. § 4.11(c) and (j). Information you provide may be used in any federal, state, or foreign civil or criminal proceeding by the Commission or other agencies.

B. **Meet and Confer:** You must contact Alain Sheer at (202) 326-3321 as soon as possible to schedule a meeting (telephonic or in person) to be held within ten (10) days after receipt of this CID in order to confer regarding your production of documents and information.

C. **Applicable time period:** Unless otherwise directed in the specifications, the applicable time period for the CID shall be from **January 1, 2007 until the date of full and complete compliance with this CID.**

D. **Claims of Privilege:** If any material called for by this CID is withheld based on a claim of privilege or any similar claim, the claim must be asserted no later than the return date of this CID. In addition, pursuant to 16 C.F.R. § 2.8A(a), submit, together with the claim, a schedule of the items withheld, stating individually as to each item:

1. the type, specific subject matter, date, and number of pages of the item;

2. the names, addresses, positions, and organizations of all authors and recipients of the item; and

3. the specific grounds for claiming that the item is privileged.

If only some portion of any responsive material is privileged, all non-privileged portions of the material must be submitted. A petition to limit or quash this CID shall not be filed solely for the purpose of asserting a claim of privilege. 16 C.F.R. § 2.8A(b).

E. **Document Retention:** You shall retain all documentary materials used in the preparation of responses to the specifications of this CID. The Commission may require the submission of additional documents at a later time during this investigation. Accordingly, you should suspend any routine procedures for document destruction and take other measures to prevent the destruction of documents that are in any way relevant to this investigation during its pendency, irrespective of whether you believe such documents are protected from discovery by privilege or otherwise. *See* 15 U.S.C. § 50; *see also* 18 U.S.C. §§ 1505, 1519. If, for any specification, there are documents that would be responsive to this CID, but they were destroyed, mislaid, transferred, deleted, altered, or over-written, describe the date and the circumstances.

F. **Petitions to Limit or Quash:** Any petition to limit or quash this CID must be filed with the Secretary of the Commission no later than twenty (20) days after service of the CID, or, if the return date is less than twenty (20) days after service, prior to the return date. Such petition shall set forth all assertions of privilege or other factual and legal objections to the CID, including all appropriate arguments, affidavits, and other supporting documentation. 16 C.F.R. § 2.7(d).

G. **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 Alain Sheer at (202) 326-3321. All such modifications must be agreed to in writing by an Associate Director, Regional Director, or

Assistant Regional Director. 16 C.F.R. § 2.7(c).

H. **Certification:** A responsible corporate officer shall certify that the response to this CID is complete. This certification shall be made in the form set out on the back of the CID form, or by a declaration under penalty of perjury as provided by 28 U.S.C. § 1746.

I. **Scope of Search:** This CID covers documents and information in your possession or under your actual or constructive custody or control including, but not limited to, documents and information in the possession, custody, or control of your attorneys, accountants, consultants, contractors, third-party providers, vendors, directors, officers, employees, and other agents, whether or not such documents were received from or disseminated to any person or entity.

J. **Document Production:** You shall produce the documentary material by making all responsive documents available for inspection and copying at your principal place of business. Alternatively, you may elect to send all responsive documents to Alain Sheer, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Mail Stop NJ-8100, Washington, D.C. 20580. 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. Notice of your intended method of production shall be given by mail or telephone to Alain Sheer at (202) 326-3321 at least five days prior to the return date.

K. **Document Identification:** Documents that may be responsive to more than one specification of this CID need not be submitted more than once; however, your response should indicate, for each document submitted, each specification to which the document is responsive. If any documents responsive to this CID have been previously supplied to the Commission, you may comply with this CID by identifying the document(s) previously provided and the date of submission. Documents should be produced in the order in which they appear in your files and without being shuffled or otherwise rearranged; if documents are removed from their original folders, binders, covers, or containers in order to be produced, then the documents shall be identified in a manner so as to clearly specify the folder, binder, cover, or container from which such documents came. In addition, number by page all documents in your submission and indicate the total number of documents in your submission. Also number all media in your submission which contain ESI and indicate the contents of the media. For media containing ESI, identify the file path where each of the individual files is located.

L. **Production of Copies:** Unless otherwise stated, legible photocopies may be submitted in lieu of original documents, provided that the originals are retained in their state at the time of receipt of this CID. Further, copies of original documents may be submitted in lieu of originals only if they are true, correct, and complete copies of the original documents; provided, however, that submission of a copy shall constitute a waiver of any claim as to the authenticity of the copy should it be necessary to introduce such copy into evidence in any Commission proceeding or court of law; and provided further that you shall retain the original documents and produce them to Commission staff upon request. 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.

M. **Submission of Electronic Data/Forms of Production**

1. The following data delivery standards outline the technical requirements for electronic document productions produced to the Federal Trade Commission. Any proposed formats other than what is listed below (including databases) should not be produced with out discussion and approval from the Litigation Support Manager of the Bureau of Consumer Protection. Submissions should be organized by custodian unless otherwise instructed. The FTC uses Concordance 9.x and Opticon 4.x to review their electronic document collections.

2. General Guidelines

   a. Documents stored in electronic or hard copy formats shall be produced as kept in the usual course of business; the FTC prefers electronically formatted productions provided that such electronic copies are true, correct, and complete copies of the original documents.

   b. Documents shall be produced in a complete form, un-redacted unless privileged, and in the order which they are kept in the Company's files in the usual course of business, inclusive of staples, clips and/or bound sections so as "re-produce" the original document delineations. For example:

      i) If in their original condition hard copy documents were stapled, clipped, or otherwise fastened together or maintained in file folders, binders, covers, or containers, they shall be reproduced in such form, and any documents that must be removed form their original folders, binders, covers, or containers in order to be produced shall be identified in a manner so as to clearly specify the folder, binder, cover or container from which such documents came.

      ii) If in their original condition electronic documents were kept in folders or otherwise organized (such as on a shared network drive or in an email program), they shall be produced in such form and information shall be produced so as to clearly specify the folder for organization format.

   c. Documents shall be produced in color where necessary to interpret the document (if the coloring of any document communicates any substantive information, of if black-and-white photocopying of conversion to TIFF format of any document (e.g., a chart or graph), makes any substantive information contained in the document unintelligible, the Company shall submit the original document, a like-colored photocopy, or a JPEG format image).

   d. If any de-duplication or email threading software or services are used when collecting or reviewing information that is stored in the Company's computer systems or electronic storage media, or the Company's computer systems contain or utilize such software, the Company shall contact Alain Sheer at (202) 326-3321.

e. A network diagram(s) depicting the Company's computer network(s) shall be produced. Typically, a network diagram will include a visual schematic identifying computer devices and communication devices within the network.

f. Microsoft Access, SQL, other databases, Microsoft Excel, and PowerPoint files shall be produced in native format with extracted text and metadata. All database productions shall include a database schema that defines the tables, the fields, relationships, views, indexes, packages, procedures, functions, queues, triggers, types, sequences, materialized views, synonyms, database links, directories, Java, XML schemas, and other elements.

g. Data compilations in Microsoft Excel or in delimited text formats shall be produced with all underlying data un-redacted and all underlying formulas and algorithms intact.

3. Scanned Collections

a. Images files – Image files shall be Group IV TIFF files (single page files). File names cannot contain embedded spaces. The number of files per folder should be limited to 5000 files.

b. Delimited Text File – This file shall contain the IMAGEID field (image key used to reference images in Opticon). The image key shall be unique, fixed length, and the same as the Bates First number of the document. The delimited text file shall include a header record. The delimiters shall be as follows:

i) Comma – ASCII character 20
ii) Quote – ASCII character 254
iii) Newline – ASCII character 174

c. Optical Character Recognition ("OCR") text – The OCR text provided to the FTC shall be delivered as a multi-page .TXT file. The name of the file shall match the IMAGEID field. Page markers shall be placed at the beginning of each OCR text page.

d. Opticon Cross-Reference File – The Opticon cross-reference file is a comma delimited file consisting of six fields per line. There shall be a cross-reference file for every image in the database. The format for the file is as follows: ImageID, VolumeLabel, ImageFilePath, DocumentBreak, FolderBreak, BoxBreak, PageCount.

i) ImageID: The unique designation that Concordance and Opticon use to identity an image.

ii) VolumeLabel: CD/DVD volume of image/OCR TXT files.

iii) ImageFilePath: The full path to the image file.

iv) DocumentBreak: If this field contains the letter "Y", then this is the first page of a document. If this field is blank, then this page is not the first page of a document.

v) Folderbreak: Leave Blank.

vi) Boxbreak: Leave Blank.

vii) PageCount: Defines the number of pages for each document.

4. Email Collections – Delimited Text with Images and Native Attachments

a. The delimited text file shall include a header record. The delimiters for the file shall be as follows:

i) Comma – ASCII character 20

ii) Quote – ASCII character 25

iii) Newline – ASCII character 174

b. The producing party shall provide a TIFF image of the email and the attachment(s), and a copy of the native attachment file(s). The text and metadata of the email and the attachment(s) shall be extracted and entered in the appropriate fields and provided as an ASCII delimited text file. All images shall be bates numbered. The email image will be the "*parent*" and the attachment(s) will be the "*child.*" An email may have more than one *child*. The *child* attachment's bates number will be listed in the *parent* email's coded fields under *CHILD_BATES*. If there is more than one attachment, list the first bates number of each attachment and separate them by semi-colons (;). The *parent* email's bates number will be listed in the *child(s)* attachment(s) under *PARENT_BATES*. The *child/children* will immediately follow the parent record. Below is a field definition table of the data requested, including hypothetical sample data:

Field	**Sample Data**	**Comment**
BEGDOC	PCC-00000001	First bates number of email
ENDDOC	PCC-00000008	Last bates number of email
BEGATTACH	PCC-00000009	First bates number of attachment(s)

ENDATTACH	PCC-00000015	Last bates number of attachment(s)
PARENT_BATES	PCC-00000001	First bates number of parent email
ATTACH_BATES	PCC-00000009, PCC-00000012	First bates number of "child" attachment(s); can be more than one bates number listed; depends on number of attachments
CUSTODIAN	Jason Wahl	Mailbox where the email resided
FROM	Jason Wahl	For email
TO	Jackie Hoel	For email
CC	Fred Thompson	For email
BCC	John McArthur	For email
EMAIL_SUBJECT	North Point Project Summary	Subject of the email
DATE_SENT	11/12/2008	Date the email was sent
TIME_SENT	04:05 PM	Time the email was sent
NATIVEFILE_LINK	D:\FTC_Production04122009 Meeting Summary\PCC-00000001.pdf	Hyperlink to native attachment (listed as file name)
DOC_EXT	.MSG, .EML, .HTML, etc.	The file extension will vary depending on whether the document is a parent email or a child attachment
AUTHOR	Jason Wahl	Attachment metadata
DATE_CREATED	11/01/2008	Attachment metadata
DATE_MOD	11/21/2008	Attachment metadata
FILE_SIZE	437,671	Attachment metadata (in KB)

PATH	K:\MGMT\SHARED\Wahl_Jason	Path where attachment file was stored
INTFILEPATH	Personal Folders/Sent Items	Location of email
TEXT	From: Wahl, Jason [PCC Corp] Sent: Tuesday, November 11, 2008 4:05 PM To: Hoel, Jackie [ABC Corp] Subject: North Point Project Summary Janice: Attached are copies of the North Point Project Summary as well as the site plan. Please let me know if you have any questions. Jason Wahl Team Lead PCC Corp 202-555-1212 - office Wahl.jason@pcccorp.com	Text of the email or attachment

5. Native Files – Native files shall be delivered with an ASCII delimited file containing the metadata associated with the files, text extracted from the native file, and a directory path to the native file. The fields to be included in the production are as follows:

FIELD	SAMPLE DATA	COMMENT
BATESFIRST	PCC-00000001	Unique sequential number
LINK	D:\SEC Production\10_01_02 Meeting Minutes\PCC-00000001.pdf	Hyperlink to native file (listed as file name)
AUTHOR	Jason Wahl	
DATE_CREATED	10/08/2009	
DATE_MOD	10/09/2009	
FILE_SIZE	765,952	
PATH	K:\MGMT\SHARED\Wahl_Jason	Path where native file was stored

CUSTODIAN	Name of the file custodian	
MD5 or SHA1	Hash Value	
Subject	Title of Document	
TEXT	Meeting Minutes for Teleconference 10/1/03 Discussion over employee stock options transpired. Decision was made to offer the options as part of the employee's Christmas bonus. Announcement was made regarding Roland Moore being promoted to Assistant Director.	Text extracted from native file

6. Media Format

a. Data may be delivered on CD, DVD, or hard drive. The media shall be encrypted. The FTC prefers to receive productions on the smallest number of media.

b. Specifications

i) Root of CD/DVD/Hard drive – two folders named Data and Images – the load files should go in the data folder and the images should go in the images folder with no more than 1000 images per folder. If you need more than one folder, please label the sub folders Vol001, Vol002, etc.

ii) CD Label shall indicate the following:

(a) Case Name
(b) Case Number
(c) Box Number
(d) Custodian Information
(e) Associated Bates Number or System Number
(f) Box(es) Source(s)
(g) CD volume

iii) Submit electronic files and images as follows:

(a) For productions over 10 gigabytes, use IDE or EIDE hard disk drives, formatted in Microsoft Windows-compatible, uncompressed data in USB 2.0 external enclosure; data shall be encrypted.

(b) For productions less than 10 gigabytes, CD-R, CD-ROM, and DVD-ROM for Windows-compatible personal computers and USB 2.0 Flash Drives are also acceptable storage formats.

iv) All documents produced in electronic format shall be scanned for and free of viruses. The FTC will return any infected media for replacement, which may affect the timing of the Company's compliance with this request.

N. **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 ways to protect such information during production. 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.

O. **Information Identification:** Each specification and sub-specification of this CID answered separately and fully in writing under oath. All information submitted shall be clearly and precisely identified as to the specifications or subspecifications to which it is responsive.

P. **Submission of Documents in lieu of Interrogatory Answers:** Previously existing documents that contain the information requested in any written Interrogatory may be submitted as an answer to the Interrogatory. In lieu of identifying documents as requested in any Interrogatory, you may, at your option, submit true copies of the documents responsive to the Interrogatory, provided that you clearly indicate the specific Interrogatory to which such documents are responsive.

Q. **Certification of Records of Regularly Conducted Activity:** Attached is a Certification of Records of Regularly Conducted Activity, which may reduce the need to subpoena the Company to testify at future proceedings in order to establish the admissibility of documents produced in response to this CID. You are asked to execute this Certification and provide it with your response.

SPECIFICATIONS

I. INTERROGATORIES

1. Identify the complete legal name of Sweetbay and all other names under which it has done or does business, its corporate mailing address, and the date and state of incorporation.

2. Identify and describe Sweetbay's parents, subsidiaries (whether wholly or partially owned), divisions (whether incorporated or not), affiliates, branches, joint ventures, franchises, operations under assumed names, websites, entities over which it exercises supervision or control. For each such entity, identify and describe the nature of its relationship to Sweetbay.

3. Identify the complete legal name of each entity that owns, operates, or otherwise controls the operation of each pharmacy located in a Sweetbay store, and for each such entity, describe in detail the nature of its relationship to Sweetbay and Hannaford.

4. Identify and describe in detail each type of pharmacy information that is created, processed, and stored when Sweetbay receives, processes, or completes a transaction in a pharmacy located in a Sweetbay store (collectively, "Sweetbay pharmacy information").

5. For each type of Sweetbay pharmacy information, identify:

   (a) the name, location, and operating system of each computer network used by or for Sweetbay to receive, process, or store the information, including, but not limited to, networks connecting to computers in store pharmacies (collectively, "HIPAA computers"), POS networks in stores, and corporate headquarter or datacenter networks;

   (b) the format in which such information is stored in computers, servers, or devices on each network, such as in clear readable text, encrypted text, or a proprietary format, and, if the information is encrypted or in a proprietary format, identify the encryption method or the proprietary format;

   (c) the complete transmission or flow path for Sweetbay pharmacy information between and within computer networks used by or for Sweetbay or Hannaford in completing transactions (starting, for example, with a request for an insurer's approval for coverage for a prescription, receipt of the approval, a request for approval to use a payment card to pay for the prescription, and ending with receipt of payment card approval), and each portion of the flow path where pharmacy information is transmitted in clear text and each point where the information is stored in clear text;

   (d) the period of time for which Sweetbay retains each type of Sweetbay pharmacy information, each application used to process or store the information, such as a pharmacy application, and individuals (by job description) or entities who have access to the information; and

   (e) the average weekly volume of pharmacy information that Sweetbay creates, processes, or stores in all of its pharmacies, including the number of unique customers the information concerns.

6. Identify and describe in detail how Sweetbay processes and stores Sweetbay pharmacy information on POS networks in its stores, setting forth specifically:

   (a) the types of information processed or stored on each POS network and the format(s) in which its is processed or stored;

   (b) the periods of time for which pharmacy information was processed or stored on the POS network;

   (c) the computer, server, or device on the network ("POS server") where pharmacy information was processed or stored and the other business functions performed by server;

   (d) where and how Sweetbay backs-up its pharmacy information, explaining whether it changed any of its back-up procedures; and

   (e) when Sweetbay pharmacy information processed or stored on the POS server was first encrypted, if ever, explaining the reasons Sweetbay encrypted the information.

7. Separately for POS networks and HIPAA computers, identify and describe in detail:

   (a) the security practices used by or for Sweetbay to prevent unauthorized access to Sweetbay pharmacy information; and

   (b) the extent to which Sweetbay or Hannaford is responsible for selecting maintaining, updating, and securing POS networks and HIPAA computers or choosing third party providers to do so. The response should include, but not be limited to: the specific responsibilities of each entity with respect to security on the POS networks and HIPAA computers by name and location; and, if Hannaford is responsible in whole or part for security, the POS networks and HIPAA computers for which it is responsible, the process by which, and frequency with which Hannaford obtains access to the network or computer, the functions it performs, and the extent of supervision by Sweetbay of Hannaford's activities.

   The responses to each subpart of this Interrogatory should describe in detail each material change or update to a security practice that relates to the subpart, as well as the date the change or update was implemented and the reasons for the change or update.

8. Identify and describe the nature of the breach as it relates to Sweetbay pharmacy information, setting forth specifically:

   (a) the security practices implemented by or for Sweetbay in response to the breach, including, but not limited to, measures taken to protect against unauthorized access to pharmacy information and other types of personal information; and

(b) the volume of pharmacy information that Sweetbay created, processed, or stored in all of its pharmacies while the breach was ongoing, including the number of unique customers the information concerns.

The responses to each subpart of this Interrogatory should describe in detail each material change or update to a security practice that relates to the subpart, as well as the date the change or update was implemented and the reasons for the change or update.

9. Identify each security audit or forensic analysis of the breach as it relates to Sweetbay pharmacy information (collectively "breach analysis"), whether prepared internally or by a third-party, describing in detail each material factual statement or assertion in each breach analysis that you dispute and explaining the bases for your position.

10. Identify and describe in detail the harms and injuries claimed by customers, putative plaintiffs, plaintiffs, law enforcement, or state Attorneys General resulting from the breach as it relates to pharmacy information, including, but not limited to, the number of government identification cards (such as driver's license or Social Security cards) and insurance cards that have been cancelled and re-issued, setting forth the costs of doing so by type of card.

11. Identify the specific goal(s) or objective(s) of each security practice (and material change thereto over the applicable time period) used to prevent unauthorized access to pharmacy and other types of personal information. Without limiting the response to the following example, a security practice could be to update and patch computer networks, devices, and applications, with the goal of successfully updating and patching a certain minimum number of computer networks, devices, and applications within a designated time period after updates or patches become available (collectively, "patching procedure").

12. Identify all Sweetbay employees, consultants, contractors, third-party providers, vendors, and other persons or entities with responsibility for information security (collectively, "responsible person"), describing in detail their qualifications and their roles and responsibilities as to each security practice and goal identified in response to Interrogatory Specification 11, and setting forth specifically:

(a) the period of time during which each responsible person performed his or her roles or responsibilities as to each security practice;

(b) the means by which Sweetbay evaluated each responsible person's performance; and

(c) whether Sweetbay disciplined, sanctioned, or imposed other adverse actions on any responsible person for reasons related in any way to the breach, identifying the responsible person sanctioned and the reasons for the adverse action; and

(d) the extent to which responsive documents from the custodial files of responsible persons identified in response to Interrogatory Specification 12 have not been produced and the reasons such documents have not been produced.

13. For each security practice and goal identified in response to Interrogatory Specification 11, identify and describe in detail:

(a) the means used to implement the security practice, the person or entity who decided on the means to be used, and the person or entity who implemented it. For example, the IT operations team could decide to use an automated patching tool to implement the patching procedure and direct a third-party provider to implement the tool;

(b) the means used to determine the extent to which the security practice's goal or objective has been achieved (collectively, "validation process"), the person or entity responsible for conducting the validation process, and the schedule for the validation process. For example, if the patching procedure uses an automated tool implemented by a third-party provider, the validation process could involve having an employee review reports generated by the tool each week and inspect a set of applications to verify that the tool is working correctly and the reports are accurate; and

(c) all results of validation processes.

14. Identify and describe in detail the reporting structure or hierarchy for each responsible person identified in the response to Interrogatory Specification 12 including the roles of management personnel and those who report to them, and provide an organizational chart.

15. Identify and describe in detail the extent of the use since 2005 of the default system administrator password ("default password") on SQL servers and applications (collectively, "SQL server") on computer networks used by or for Sweetbay. The response should include, but not be limited to:

(a) a table that identifies for each SQL server: the name of the server; the name and address of the store or other location where the server (was or) is located; how the server was used (such as to process payment card transactions or store pharmacy information); the name of the vendor providing the server; the server's default password; the application(s) used, by name and version; the period of time during which the default password was used on the server, how frequently it was used, and the purpose(s) for which it was used; the person(s) responsible for the decision to use the default password after the server had been installed on a network; and the person(s) who used the password, such as a vendor or a Sweetbay or Hannaford employee;

(b) a detailed explanation of why the default password was not changed after the server was installed, such as to prevent a loss of functionality that would occur if the default password were changed, and Sweetbay's or Hannaford's efforts to change the server or application so that using the default password would not be necessary to avoid losing functionality; and

(c) an explanation of other security measures used in lieu of changing the default password on each server.

16. Identify and describe in detail the extent of the use of the xp_cmdshell function on SQL servers and applications (collectively, "SQL server") on computer networks used by or for Sweetbay. The response should include, but not be limited to:

(a) a table that identifies for each SQL server on which xp_cmdshell functionality was enabled (in whole or part): the name of the server; the name and address of the store or other location where the server was (or is) located; how the server was used (such as to process payment card transactions or store pharmacy information); the period of time during which the functionality was enabled, how frequently it was used, and the purpose(s) for which it was used; the person(s) responsible for the decision to enable the functionality; and the person(s) who used the functionality, such as a vendor or a Sweetbay or Hannaford employee; and

(b) an explanation of other security measures used in lieu of disabling xp_cmdshell functionality.

17. Separately for POS networks and HIPAA computers, identify and describe in detail each administrative or other computer network account used by or for Sweetbay to manage the networks and computers. For each such account, the response should include, but not be limited to:

(a) all functions that can be performed with the account, and the networks, computers, servers, devices, and applications to which the account provides access or control, and the extent of such access or control;

(b) the date when the account was first created;

(c) the account's configuration (such as the default configuration), whether logins to the account are automatically recorded, the dates when the account has been used, the purposes it was used for, and the person(s) who used the account, such as a vendor or an employee of Sweetbay or Hannaford; and

(d) information about whether the account was ever disabled, and, if so, why, when, and for what period, and if not, why not.

18. Identify and describe in detail whether and, if so, how and why computers, servers, and devices on POS networks in Sweetbay stores could connect directly to the internet.

19. Identify and describe in detail each marketing or promotional activity (collectively, "promotion") you undertook in response to the breach, such as providing discount coupons, gift cards, or other benefits to customers, identifying for each such promotion: the target group (such as customers who expressed concern about the breach, customers whose personal information was or may have been exposed through the breach, or other customers and employees or prospective employees); the purpose of the promotion; the cost of the promotion; the number of customers or employees who received the promotion; and any assessment of the promotion's effectiveness in achieving its purpose.

20. Identify and describe in detail whether, and, if so, how and over what time period, customers of Sweetbay changed their purchasing practices after the breach was announced, including, but not limited to, changes in:

    (a) the form of payment used (such as switching from payment cards to cash and checks);

    (b) the average dollar amount of purchases by payment form; and

    (c) the churn rate or attrition rate in Sweetbay's customer base, reflecting the proportion of customers who stopped doing business with Sweetbay.

    The response should include, but not be limited to: a spreadsheet that sets out, week-by-week between March 17, 2007 and March 17, 2009, changes in the form and average dollar amount of customer payment (by individual form of payment) and the churn rate (by demographic characteristics and location); the raw data upon which each spreadsheet is based; and a detailed description of the methods used to prepare each spreadsheet.

21. Do you contend that no payment card, pharmacy information, or other personal information of customers was taken from Sweetbay through the breach? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts, identify all witnesses, and identify all documents on which you base the qualification.

22. Do you contend that no action taken by the intruder in conducting the breach triggered a warning of anomalous or unauthorized network activity from security devices and services operated by or for Sweetbay? If so, describe all facts, identify all witnesses, and identify all documents on which you base your contention. If your response is anything other than an unqualified yes, describe all facts (including the types and number of warnings that were triggered, when they were triggered, and any responses thereto), identify all witnesses, and identify all documents on which you base the qualification.

23. Identify the custodians, sources, and physical locations of all information responsive to

all Specifications of this CID, describing in detail the tools and methodologies you used to identify and locate responsive information.

II. DOCUMENTS

1. Provide all documents prepared by or for Sweetbay that identify, describe, investigate, evaluate, or assess: (a) how the breach occurred; (b) the time period over which it occurred; (c) where the breach began (*e.g.*, what the point of entry was and whether it was located in a store or on a central network linking stores); (d) the path the intruder followed from the point of entry to the information compromised and then in exporting or downloading the information (including all intermediate steps); and (e) the types and amounts of information that were or may have been accessed without authorization.

   Responsive documents should include, but not be limited to: preliminary, interim, draft, and final reports that describe, assess, evaluate, or test security vulnerabilities that were or could have been exploited in the breach; reports of penetration and gap analysis; logs that record the intruder's steps in conducting the intrusion; warnings issued by anti-virus, intrusion detection, or other security measures; records of the configuration of applications, programs, and network components used in card authorization (such as whether an application was misconfigured to store or record transactions); records setting out reviews by network administrators or others to verify that newly created user accounts were authorized; security scans (such as for packet capture tools, password harvesting tools, rootkits, and other unauthorized programs); incident reports; (formal and informal) security audits or forensic analyses of the breach prepared internally and by third-parties; and other records relating or referring to the breach, including minutes or notes of meetings attended by Sweetbay personnel and documents that identify the attackers.

2. For each network identified in response to Interrogatory Specification 5(a), provide:

   (a) blueprints and diagrams setting out in detail the components, topology, and architecture of the network. Responsive documents should include, but not be limited to, documents that identify and locate the components of the network, such as: computers; POS devices; cash registers; remote access equipment (such as wireless access points); servers; firewalls; routers; internet, private line, and other connections; connections to other Sweetbay networks and outside networks; and security mechanisms and devices (such as intrusion detection systems);

   (b) documents setting out the security practices used to protect pharmacy information from unauthorized access while created, processed, or stored within a network or between networks;

   (c) documents sufficient to set forth the complete transmission or flow path for Sweetbay pharmacy information between and within computer networks used by or for Sweetbay or Hannaford in completing transactions (starting, for example, with a request for an insurer's approval for coverage for a prescription, receipt of the approval, a request for approval to use a payment card to pay for the prescription, and ending with receipt of payment card approval), and each portion of the flow path where pharmacy information is transmitted in clear text and each point where the information is stored in clear text; and

(d) documents that refer to security vulnerabilities in the networks, including, but not limited to, documents identifying vulnerabilities, documents setting out and explaining the measures implemented to address the vulnerabilities, and communications, such as emails, that assess, question, or describe the state of security, warn of vulnerabilities, or propose or suggest changes in security measures.

3. Provide all communications with companies providing information security products and services to Sweetbay, including, but not limited to, communications with BigFix, or any third-party provider or vendor monitoring or servicing BigFix's patch-management product.

4. Provide documents sufficient to identify the time line followed in implementing critical (or equivalent) updates and patches on Sweetbay computer networks, computers, servers, devices, and applications, including, for each entity, when an update or patch became available, when it was implemented, and the extent of its implementation across networks, computers, servers, devices, and applications.

5. Provide a copy of each substantially different access control list used to control access to Sweetbay networks, computers, servers, devices, and applications (collectively, "resources"), and provide documents that identify the name and the location of each resource to which each access control list applies, and when, how, and why changes, if any, were made to the access control list. The response should include, but not be limited to, access control lists that apply to border routers and firewalls, POS networks, store VLANs, and Hannaford's corporate environment.

6. Provide all documents that relate to the use of the system administrator password, including the default password, since 2005 on SQL servers and applications (collectively, "SQL server") on computer networks used by of for Sweetbay. The response should include, but not limited to:

(a) documents sufficient to identify for each SQL server: the name of the server; the name and address of the store or other location where the server (was or) is located; how the server was used (such as to process payment card transactions or store pharmacy information); the name of the vendor of the server; the server's default password; the application(s) used, by name and version; the period of time during which the default password was used on the server, how frequently it was used, and the purpose(s) for which it was used; the person(s) responsible for the decision to use the default password after the server had been installed on a network; and the person(s) who used the password, such as a vendor or a Hannaford employee;

(b) all communications with vendors and service providers about any loss of functionality resulting from changing the default password, including requests to modify the server or applications to prevent the functionality loss;

(c) all communications with acquiring banks regarding system administrator passwords used on servers identified in the response to Document Specification 6 (a);

(d) all communications with a card association or the Payment Card Industry Data Security Council regarding system administrator passwords used on servers identified in the response to Document Specification 6(a);

(e) all communications within Sweetbay or between Sweetbay and any other person or entity regarding the use of system administrator passwords on servers identified in the response to Document Specification 6(a), including the consequences of using the default system administrator password; and

(f) documents that identify other security measures used in lieu of changing the default password.

7. Provide all documents that relate to the use of the xp_cmdshell function on SQL servers and applications (collectively, "SQL server") on computer networks used by Sweetbay. The response should include, but not be limited to:

(a) documents sufficient to identify for each SQL server: the name of the server; the name and address of the store or other location where the server was (or is) located; how the server was used (such as to process payment card transactions or store pharmacy information); the period of time during which xp_cmdshell functionality was enabled, how frequently it was used, and the purpose(s) for which it was used; the person(s) responsible for the decision to enable the functionality; and the person(s) who used the functionality, such as a vendor or a Sweetbay or Hannaford employee;

(b) all communications with acquiring banks regarding xp_cmdshell functionality on servers identified in the response to Document Specification 7(a);

(c) all communications with a card association or the Payment Card Industry Data Security Council regarding xp_cmdshell functionality on servers identified in the response to Document Specification 7(a);

(d) all communications within Sweetbay or between Sweetbay and any other person or entity regarding the use of xp_cmdshell functionality on servers identified in the response to Document Specification 7(a); and

(e) documents that identify other security measures used in lieu of disabling xp_cmdshell.functionality.

8. Provide all documents that relate to administrative or computer network accounts used to manage or update the POS networks. Separately for each account, the response should include, but not be limited to:

(a) all functions that can be performed with the account, and the networks, devices, and applications to which the account provides access or control and the extent of such access or control;

(b) the date when the account was first created;

(c) the account's configuration (such as the default configuration), whether logins to the account are automatically recorded, the dates when the account has been used, the purposes it was used for, and the person(s) who used the account, such as a vendor or an employee of Sweetbay or Hannaford; and

(d) information about whether the account was ever disabled, and, if so, why, when, and for what period, and if not, why not.

9. Starting in 2005, provide all documents, prepared by or for Sweetbay that question, challenge, or dispute the effectiveness of, or recommend changes to, security practices implemented on networks identified in the response to Interrogatory Specification 5(a), and all responses thereto.

10. Without redacting personal information, provide a copy of a file that is representative of the types, and format, of pharmacy information that is stored on Sweetbay POS networks.

11. Provide copies of documents settling claims and/or reimbursing claims for costs related to the breach.

12. For the period March 17, 2007 through March 17, 2009, provide all documents that describe, evaluate, or analyze the purchasing practices of Sweetbay's customers, including, but not limited to, documents that concern changes in the form of payment, the average dollar amount of purchases (by individual form of payment), and the churn rate (by demographic characteristics and location); and the underlying data, analytical methodology, and conclusions.

13. Provide all documents on which you base your responses to Interrogatory Specifications 21 and 22.

14. Provide the documents on which you base the responses to all the foregoing Interrogatories.

CERTIFICATION OF RECORDS OF REGULARLY CONDUCTED ACTIVITY
Pursuant to 28 U.S.C. § 1746

1. I, ____________________________, have personal knowledge of the facts set forth below and am competent to testify as follows:

2. I have authority to certify the authenticity and accuracy of the records produced by Kash n' Karry Food Stores, Inc. and attached hereto.

3. The documents produced and attached hereto by Kash n' Karry Food Stores, Inc. are originals or true copies of records of regularly conducted activity that:

   a) Were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person with knowledge of those matters;

   b) Were kept in the course of the regularly conducted activity of Kash n' Karry Food Stores, Inc.; and

   c) Were made by the regularly conducted activity as a regular practice of Kash n' Karry Food Stores, Inc.

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

Executed on ____________________, 2010.

____
Signature