EXHIBIT 12

HANNAFORD BROS. CO.'S OBJECTIONS TO THE FEDERAL TRADE COMMISSION'S FIRST CIVIL INVESTIGATIVE DEMAND (THE "WHITE PAPER CID")[1]

Pursuant to 15 U.S.C. § 57b-1(b)(13), Hannaford Bros. Co. ("Hannaford"), by and through its undersigned counsel, provides its objections to the first Civil Investigative Demand ("CID") of the Federal Trade Commission dated November 2, 2010 and served on November 5, 2010.

General Objections

1. Hannaford objects to the CID as overbroad and unduly burdensome.

2. Hannaford objects to the CID to the extent that it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, the common interest privilege, the self-evaluative privilege, or any other applicable privilege or immunity.

3. Hannaford objects to the CID to the extent that it seeks the disclosure of information or production of documents that are confidential.

4. Hannaford objects to the CID to the extent it seeks information or documents beyond the scope of, or seeks to impose obligations on Hannaford beyond those authorized by, the Resolutions attached to the CID.

5. Hannaford objects on the grounds that the Resolution attached to the CID Directing the 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

[1] By letters dated November 23, 2010 and December 10, 2010, the FTC agreed to narrow certain aspects of this CID. These objections are based on the CID as narrowed by those letters. Hannaford reserves the right to revise these objections if the FTC determines not to narrow the CID as set forth in its letters. In its letters, the FTC has referred to this CID as the "White Paper CID."

Gramm-Leach-Bliley Act ("GLBA") and/or Section 5 of the FTC Act (File No. 002-3284) is not specifically related to the FTC's investigation of Hannaford and is not sufficient to authorize this CID.

6. Hannaford objects on the grounds that the Resolution attached to the CID Directing Use of Compulsory Process in a 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. sec.* (the Fair Credit Reporting Act or "FCRA") and/or 15 U.S.C. § 45 (File No. 992-3120) is not specifically related to the FTC's investigation of Hannaford and is not sufficient to authorize this CID.

7. Hannaford objects to the CID to the extent it seeks information or documents over which Hannaford does not have possession, custody, or control.

8. Hannaford objects to the CID to the extent it seeks information or documents the disclosure of which violates consumer or employee privacy rights.

9. Hannaford objects to the CID to the extent it seeks the disclosure of information or documents that contain health information protected under the Health Insurance Portability and Accountability Act ("HIPAA") pursuant to 42 U.S.C. § 201 *et. seq.*, 45 C.F.R. § 164.530(i), and 45 C.F.R. §§ 164.316(a).

10. Hannaford objects to the CID insofar as it includes "contention" interrogatories, which are premature at the investigative stage and are appropriate only after discovery in litigation.

11. The following specific objections fully incorporate, are subject to, and are made without waiver of the foregoing general objections.

Objections to Definitions

1. Hannaford objects to Definition G of "Electronically Stored Information" or "ESI" as unduly burdensome insofar as it requires Hannaford to collect and recover, restore, or produce ESI that exists on backup media or in other forms that are not reasonably accessible.

2. Hannaford objects to Definition J of "Hannaford" or "Company" as ambiguous because the term "agents" is vague and could be read to seek information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity.

3. Hannaford objects to Definition M of "personal information" as overbroad and irrelevant because it includes information about employees, not just "consumers."

4. Hannaford objects to Definition Q of "security practice" as overbroad because it defines the term to include more than technological and computer network security, and can be read to encompass door locks, facility cameras, and other non-technological or non-computer-related security.

Objections to Instructions

1. Hannaford objects to Instruction D of the CID as unduly burdensome because it requires Hannaford to catalogue and provide a voluminous amount of information in its privilege log and because the time frame provided for preparing and producing a privilege log is too short.

2. Hannaford objects to Instruction E of the CID as unduly burdensome and overbroad because the term "in any way relevant" can be read to apply to an unmanageable volume of documents or to documents that do not contain unique, relevant information. Hannaford further objects to this instruction to the extent it differs from, or seeks to enlarge, Hannaford's preservation obligations beyond those provided under the applicable federal law.

3. Hannaford objects to Instruction I of the CID to the extent it seeks the disclosure of information or production of documents subject to the attorney-client privilege and/or the work product privilege, the common interest privilege, the self-evaluative privilege, or other applicable privileges and immunities.

4. Hannaford objects to Instruction K of the CID as unduly burdensome because it requires Hannaford to identify for each document which specification(s) or subspecification(s) to which it responds.

5. Hannaford objects to Instruction L of the CID on the grounds that it instructs that producing a copy of a responsive document constitutes a waiver of any claim as to the authenticity of the document.

6. Hannaford objects to Instruction M.2 of the CID because it is ambiguous as to the format for production.

7. Hannaford objects to Instruction M.4 of the CID as unduly burdensome because it appears that the BEGDOC field for emails is supposed to contain the same data as the BATESFIRST field for native files, making production more burdensome than if these fields had uniform names.

8. Hannaford objects to Instruction M.4 of the CID as vague and unduly burdensome because it appears that the field PATH asks for the location where an email attachment was stored, before it was attached to the email. Hannaford does not have that information.

9. Hannaford objects to Instruction N of the CID because it appears to contemplate the production of personal health information that is protected by HIPAA.

10. Hannaford objects to Instruction O of the CID as unduly burdensome because it requires to Hannaford to identify for each piece of information the specification(s) or subspecification(s) to which it responds.

Objections to 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").

Objection: Hannaford objects to this interrogatory as vague because the terms "security practice" and "material change" are ambiguous. Hannaford further objects to this interrogatory as overbroad because the term "security practice" is defined to include more than technological and computer network security. Hannaford further objects on the grounds that the interrogatory is unduly burdensome because it would require Hannaford to analyze a voluminous amount of information.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* individuals and entities described. Hannaford also objects on the grounds that the interrogatory is ambiguous because the terms "information security," "security practice," "the means by which Hannaford evaluated each responsible person's performance," and "adverse actions" are vague. Hannaford further objects to this interrogatory as overbroad because the term "security practice" is defined to include more than technological and computer network security. Hannaford further objects on the grounds that the interrogatory is unduly burdensome because it would require Hannaford to analyze a voluminous amount of information. Hannaford also objects to this Hannaford as overbroad because it seeks information not in the possession, custody, or control of Hannaford. Finally, Hannaford also objects to the interrogatory to the extent that it seeks the disclosure of information or production of documents

subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity.

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.

   Pursuant to the FTC's letter of November 23, 2010, the time period for this specification is modified to begin on January 1, 2007 and end on January 1, 2009.

Objection: Hannaford objects to this interrogatory as overbroad because the term "security practice" is defined to include more than technological and computer network security.

Hannaford further objects on the grounds that the interrogatory is unduly burdensome because it would require Hannaford to analyze a voluminous amount of information. Hannaford further objects to this interrogatory because it seeks information not in the possession, custody, or control of Hannaford.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it will require Hannaford to analyze a voluminous amount of information given the normal personnel changes Hannaford has experienced over the period of time covered by this CID. It further objects to the interrogatory insofar as it seeks information not in the possession, custody, or control of Hannaford. Finally, Hannaford also objects to this interrogatory because it incorporates Interrogatory Specification 2, which is overbroad, unduly burdensome, vague, and insofar as it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity, as set forth above.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it seeks information for every change that is logged. It further objects to the interrogatory as ambiguous because the terms "SQL servers and applications," "extent of the use," "default password," and "other security measures" are vague. It also objects to the interrogatory as overbroad because the interrogatory seeks information about the use of default passwords on "SQL servers" on the computer networks of Hannaford, Sweetbay, and Shop 'n Save when not all servers on their computer networks were implicated in the intrusion.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it would require Hannaford to analyze a voluminous amount of information. Hannaford further objects to this interrogatory as ambiguous because the term "material differences" is vague. Hannaford also objects to this interrogatory as overbroad because the term "security practice" is defined to include more than technological and computer network security. Hannaford further objects to

the interrogatory as irrelevant because there was no compromise of pharmacy information. Hannaford also objects insofar as the interrogatory seeks information about employees, and not just consumers.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome. Hannaford further objects to this interrogatory as ambiguous because the terms "marketing or promotional activity" and "effectiveness in achieving its purpose" are vague. It further objects on the basis that reference to "marketing or promotional activity" in this context is a mischaracterization and argumentative.

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: (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: 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.

Objection: Hannaford objects to this interrogatory as unduly burdensome. It also objects to the interrogatory as ambiguous overall, and specifically because the term "churn rate" is vague, what it means for a customer to change his or her purchasing practices is vague, and because the term "demographic characteristics" is vague. It further objects to the interrogatory on the basis that it is speculative. Hannaford also objects to the interrogatory as overbroad and seeking irrelevant information because whether or how customers of Hannaford, Sweetbay, or Shop 'n Save may have "changed their purchasing practices" after March 17, 2008 may have nothing to do with the intrusion, particularly because the intrusion occurred in the midst of a recession. It further objects because some of the information, such as the demographics of certain customers who pay with cash, is not within Hannaford's control.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome. It further objects because it will be difficult, if not impossible, to quantify "the impact of the breach" on Hannaford's sales revenue.

10. Separately for 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)

Objection: Hannaford objects to this interrogatory as unduly burdensome and as seeking irrelevant information.

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.

Objection: None. Hannaford assumes the document referenced in this interrogatory is the electronic file produced in native format and labeled HAN-009641.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome. Hannaford also objects to the interrogatory as ambiguous because the term "pharmacy information" is vague. Hannaford further objects to the interrogatory as irrelevant because there was no compromise of pharmacy information. It further objects to the interrogatory as seeking information beyond the purported scope of the Resolutions attached to the CID.

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.

Objection: None.

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 qualifications.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It objects on the basis that the interrogatory is ambiguous because the terms "systematic data classification and inventory process" and "material changes" are vague. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. Hannaford also objects to this interrogatory as vague because the term "administrative level accounts" is ambiguous. It also objects on the grounds that this "contention" interrogatory is premature and is

appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. Hannaford also objects to this interrogatory as ambiguous because the terms "administrative level accounts" and "in the same domain in which the POS servers were members" are vague and the inquiry overall is ambiguous. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as ambiguous because the terms "readily available measures" and "material" are vague. It further objects because the interrogatory calls for a legal conclusion. It also objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as ambiguous because the term "any material respect" is vague. Hannaford also objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate

only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as ambiguous because "at any time during the breach" is vague. Hannaford further objects on the grounds that the interrogatory is irrelevant because it seeks information about employees and not consumers. It also objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. Hannaford also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. Hannaford also objects to the interrogatory as ambiguous because the terms "at any time during the breach" and "pharmacy transactions" are vague. Hannaford also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative. Hannaford further objects to the interrogatory as irrelevant because there was no compromise of pharmacy information.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue and because it would require talking to all current and former Hannaford employees about their knowledge of PCI and "compensating controls." It also objects to the interrogatory as ambiguous and virtually incomprehensible overall, and because the terms "[s]etting aside compensating controls that could bring an entity into compliance with a PCI DSS requirement that otherwise would not be satisfied" and "prior to and while the breach was ongoing" are vague, and because "compensating controls" are an integral part of the PCI DSS and cannot be "set aside." It also objects to the interrogatory's request for Hannaford to certify that "no Hannaford employee had actual knowledge that Hannaford had not fully satisfied each requirement and subpart of the PCI DSS" as unduly burdensome and vague. Hannaford also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation

interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome and overbroad.

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.

Objection: Hannaford objects to this document specification as unduly burdensome and overbroad because is it seeking *all* documents related to this issue. Hannaford further objects because this document specification is seeking documents subject to the attorney-client privilege and the work product privilege. Hannaford also objects to this specification as overbroad because the term "security practice" is defined to include more than technological and computer network security. Hannaford further objects on the grounds that this document specification is unduly burdensome because it would require Hannaford to review and produce a voluminous number of documents. Finally, Hannaford objects to this request because it seeks documents not in its possession, custody, or control.

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.

Objection: Hannaford objects to this document specification as unduly burdensome and overbroad. It further objects to the document specification as ambiguous because the terms "sufficient to identify," "time line followed," and "critical (or equivalent)" are vague.

3. Separately for Hannaford, Sweetbay, and Shop 'n Save, provide:

   (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.

Objection: Hannaford objects to this document specification as overbroad and unduly burdensome because it seeks information for every change that is logged and because it seeks *all* communications. It also objects to the specification insofar as it seeks documents subject to the attorney-client privilege and the work product privilege.

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.

Objection: Hannaford objects to this document specification as overbroad and unduly burdensome because it seeks *all* documents and materials on the issue. It further objects to this document specification as ambiguous overall and because the term "effort to persuade VeriSign to make changes" is vague and improperly assumes facts. Hannaford also objects to this specification as seeking documents not in its possession, custody, or control. Finally, it objects to this specification as duplicative of document specification 1.

5. For the period March 17, 2007 through March 17, 2009, provide all documents that describe, evaluate, or analyze changes in the purchasing practices of Hannaford's customers, including 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 provide the underlying data, analytical methodology, and conclusions.

Objection: Hannaford objects to this document specification as overbroad and unduly burdensome because it seeks *all* documents on the issue. It further objects to the document specification as ambiguous overall, and specifically because the terms "churn rate" and "demographic characteristics" are vague. It objects to the document specification as overbroad and seeking irrelevant documents because *all* documents that "describe, evaluate, or analyze changes in the purchasing practices of Hannaford's customers" could include such documents as marketing studies about changes in peak shopping times and changes in the most popular breakfast cereals.

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.

Objection: Hannaford objects to this document specification as ambiguous because the term "sufficient to identify" is vague. Hannaford also objects to this specification as duplicative insofar as it seeks documents identical to information requested in Interrogatory 13 and is, therefore, unnecessary.

7. Provide documents sufficient to show all individual components, and the percentage thereof, that constitute actual or prospective acquiring banks' payment card transaction

fees, including security or PCI compliance, and provide all contracts between Hannaford and its acquiring banks.

Objection: Hannaford objects to this document specification as ambiguous because the term "sufficient to show" is vague. Hannaford also objects to this document specification as overbroad because it seeks documents about the payment card transaction fees of prospective acquiring banks, whether Hannaford has a contract with the acquiring bank. It also objects on the grounds that this specification seeks irrelevant information.

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. Pursuant to the FTC's letter of November 23, 2010, the time period for this specification is modified to begin on January 1, 2007 and end on April 1, 2008.

Objection: Hannaford objects to this document specification as vague because the meaning of the phrase "representative of the types and format of pharmacy information" is ambiguous and the meaning of the term "other devises" is also ambiguous. Hannaford also objects on the grounds that this document specification seeks the production of personal health information that is protected by HIPAA. To the extent that the FTC is attempting to use the FCRA's provision concerning medical information as a basis to seek this information, Hannaford reiterates its objection that it is not a consumer reporting agency covered by that statute. Hannaford further objects to the document specification as irrelevant because there was no compromise of pharmacy information.

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

Objection: The FTC has withdrawn this document specification, pursuant to its November 23, 2010 letter. Hannaford reserves the right to assert objections to this document specification if the FTC reinstates this specification.

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

Objection: Hannaford objects to this document specification as unduly burdensome and as seeking information beyond the purported scope of the Resolutions attached to the CID. Hannaford also incorporates each of its objections to all the foregoing interrogatories to this document specification.

HANNAFORD BROS. CO.'S OBJECTIONS TO THE FEDERAL TRADE COMMISSION'S SECOND CIVIL INVESTIGATIVE DEMAND (THE "ACCESS LETTER CID")[1]

Pursuant to 15 U.S.C. § 57b-1(b)(13), Hannaford Bros. Co. ("Hannaford"), by and through its undersigned counsel, provides its objections to the second Civil Investigative Demand ("CID") of the Federal Trade Commission dated November 2, 2010 and served on November 5, 2010.

General Objections

1. Hannaford objects to the CID as overbroad and unduly burdensome.

2. Hannaford objects to the CID to the extent that it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, the common interest privilege, the self-evaluative privilege, or any other applicable privilege or immunity.

3. Hannaford objects to the CID to the extent that it seeks the disclosure of information or production of documents that are confidential.

4. Hannaford objects to the CID because as a grocery retailer, Hannaford is not engaged in activities governed by the Gramm-Leach-Bliley Act ("GLBA").

5. Hannaford objects to the CID because as a grocery retailer, Hannaford is not engaged in activities governed by the Fair Credit Report Act ("FCRA").

[1] By letters dated November 23, 2010 and December 10, 2010, the FTC agreed to narrow certain aspects of this CID. These objections are based on the CID as narrowed by these letters. Hannaford reserves the right to revise these objections if the FTC determines not to narrow the CID as set forth in its letters. In its letters, the FTC has referred to this CID as the "Access Letter CID."

6. Hannaford objects to the CID to the extent it seeks information or documents beyond the scope of, or seeks to impose obligations on Hannaford beyond those authorized by, the Resolutions attached to the CID.

7. Hannaford objects on the grounds that the Resolution attached to the CID Directing the 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) is not specifically related to the FTC's investigation of Hannaford and is not sufficient to authorize this CID.

8. Hannaford objects on the grounds that the Resolution attached to the CID Directing Use of Compulsory Process in a 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. sec.* and/or 15 U.S.C. § 45 (File No. 992-3120) is not specifically related to the FTC's investigation of Hannaford and is not sufficient to authorize this CID.

9. Hannaford objects to the CID to the extent it seeks information or documents over which Hannaford does not have possession, custody, or control.

10. Hannaford objects to the CID to the extent it seeks information or documents the disclosure of which violates consumer or employee privacy rights.

11. Hannaford objects to the CID to the extent it seeks the disclosure of information or documents that contain health information protected under the Health Insurance Portability and Accountability Act ("HIPAA") pursuant to 42 U.S.C. § 201 *et. seq.*, 45 C.F.R. § 164.530(i), and 45 C.F.R. §§ 164.316(a).

12. Hannaford objects to the CID insofar as it includes "contention" interrogatories, which are premature at the investigative stage and are appropriate only after discovery in litigation.

13. Hannaford objects to the CID because it purports to be duplicative of prior voluntary access letters yet significantly expands the relevant time period for those earlier requests.

14. Hannaford objects to the CID because it has already provided responses to these specifications pursuant to the FTC's voluntary access letters.

15. The following specific objections fully incorporate, are subject to, and are made without waiver of the foregoing general objections.

Objections to Definitions

1. Hannaford objects to Definition H of "Electronically Stored Information" or "ESI" as unduly burdensome insofar as it requires Hannaford to collect and recover, restore, or produce ESI that exists on backup media or in other forms that are not reasonably accessible.

2. Hannaford objects to Definition K "Hannaford" or "Company" as ambiguous because the term "agents" is vague and could be read to seek information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity.

Objections to Instructions

1. Hannaford objects to Instruction E of the CID as unduly burdensome because it requires Hannaford to catalogue and provide a voluminous amount of information in its privilege log and because the time frame provided for preparing and producing a privilege log is too short.

2. Hannaford objects to Instruction F of the CID as overbroad and unduly burdensome because the term "in any way relevant" can be read to apply to an unmanageable volume of documents or to documents that do not contain unique, relevant information. Hannaford further objects to this instruction to the extent it differs from, or seeks to enlarge, Hannaford's preservation obligations beyond those provided under the applicable federal law.

3. Hannaford objects to Instruction J of the CID to the extent it seeks the disclosure of information or production of documents subject to the attorney-client privilege and/or the work product privilege, the common interest privileged, the self-evaluative privilege, or other applicable privileges and immunities.

4. Hannaford objects to Instruction L of the CID as unduly burdensome because it requires Hannaford to identify for each document which specification(s) or subspecification(s) to which it responds.

5. Hannaford objects to Instruction M of the CID on the grounds that it instructs that producing a copy of a responsive document constitutes a waiver of any claim as to the authenticity of the document.

6. Hannaford objects to Instruction N.2 of the CID because it is ambiguous as to the format for production.

7. Hannaford objects to Instruction N.4 of the CID as unduly burdensome because it appears that the BEGDOC field for emails is supposed to contain the same data as the BATESFIRST field for native files, making production more burdensome than if these fields had uniform names.

8. Hannaford objects to Instruction N.4 of the CID as vague and unduly burdensome because it appears that the field PATH asks for the location where an email attachment was stored, before it was attached to the email. Hannaford does not have that information.

9. Hannaford objects to Instruction O of the CID because it appears to contemplate the production of personal health information that is protected by HIPAA.

10. Hannaford objects to Instruction P of the CID as unduly burdensome because it requires to Hannaford to identify for each piece of information the specification(s) or subspecification(s) to which it responds.

Objections to Specifications

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.

Objections: Hannaford objects to this interrogatory as vague because the term "complete legal name" is ambiguous.

2. Identity 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.

Objections: Hannaford objects to this interrogatory as overbroad and seeking irrelevant information. Hannaford further objects because Hannaford's parent corporation is not implicated in the investigation, is a foreign corporation outside of the FTC's jurisdiction, and is not a party to these proceedings.

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.

Objections: Hannaford objects to this interrogatory on the grounds that the phrase "store, maintain, process, transmit, handle, or otherwise use (collectively hereinafter, 'store and process') personal information" is ambiguous.

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.

Objections: Hannaford objects to this interrogatory as overbroad and unduly burdensome. Hannaford also objects to this interrogatory as vague because the term "material change or update" is ambiguous. Hannaford also objects on the grounds that it incorporates interrogatory 3, which is also vague and ambiguous, as set forth above.

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.

Objections: Hannaford objects to this interrogatory as ambiguous because the terms "2007 upgrades" and "encryption practices" are vague.

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

Objections: None.

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.

Objections: Hannaford objects to the interrogatory as vague because the term "substantively different" is ambiguous.

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.

Objections: None.

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.

Objections: Hannaford objects to this interrogatory as unduly burdensome because it seeks a voluminous amount of information about multiple networks, countless components of those networks, and the continual changes being made to them. It also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information. Hannaford further objects to this interrogatory as ambiguous because the terms "components of the network," "pharmacy information," "material change" and "complete legal name" are vague.

To the extent that the FTC is attempting to use the FCRA's provision concerning medical information as a basis to seek this information, Hannaford reiterates its objection that it is not a consumer reporting agency covered by that statute. Hannaford further objects to the interrogatory as overbroad because there is no evidence that many of these networks for which it seeks information were in any way compromised. Hannaford also objects to this interrogatory to the extent it seeks information or documents over which Hannaford does not have possession, custody, or control. Finally, it objects to the request for contact information for Hannaford employees, who should be contacted through counsel.

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.

Objections: Hannaford objects to this interrogatory as unduly burdensome, overbroad, and irrelevant. There is no evidence that many of these servers for which it seeks information were in any way compromised. Hannaford also objects to the interrogatory as ambiguous because the term "pharmacy information" is vague. It also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

To the extent that the FTC is attempting to use the FCRA's provision concerning medical information as a basis to seek this information, Hannaford reiterates its objection that it is not a consumer reporting agency covered by that statute.

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.

Objections: Hannaford objects to this interrogatory as unduly burdensome, overbroad, irrelevant, and not reasonably calculated to lead to the discovery of admissible evidence. There is no evidence that many of the systems, networks, and computers for which it seeks information were in any way compromised.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome, overbroad, and irrelevant because it appears to seek information related to activities of a financial institution within the meaning of the GLBA and activities of consumer reporting agency within the meaning of the FCRA, when the GLBA and FCRA do not apply to Hannaford. Hannaford also objects to this interrogatory as ambiguous because the terms "processing electronic payment transactions," "check collection and processing services," "automated clearinghouse processing," "network services," and "settlement services" are vague.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome, overbroad and irrelevant because the GLBA and FRCA do not apply to Hannaford. Hannaford also objects to this interrogatory as vague because the terms "components and operation of the service," "annual revenue," and "cost savings" are ambiguous. Hannaford also objects to this interrogatory and on the grounds that it refers to interrogatory 12, which is unduly burdensome, overbroad, irrelevant, vague, and ambiguous, as set forth above.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it seeks an analysis of voluminous information. Hannaford also objects to this interrogatory as vague because the terms "payment processing and related services" and "component of the services" are ambiguous.

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.

Objection: Hannaford objects to this interrogatory as overbroad and unduly burdensome because it seeks an analysis of voluminous information. Hannaford also objects to this interrogatory as irrelevant because the GLBA does not apply to Hannaford.

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.

Objection: Hannaford objects to this interrogatory as irrelevant because Hannaford is not a consumer reporting agency within the meaning of the FCRA. Hannaford also objects to this interrogatory as vague because the term "policies and procedures to ensure compliance with Section 615(a) of the FCRA" is ambiguous. Hannaford further objects because this interrogatory is unduly burdensome.

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).

Objection: Hannaford objects to this interrogatory as irrelevant because Hannaford is not a consumer reporting agency within the meaning of the FCRA and it is not a financial institution within the meaning of the GLBA. Hannaford also objects on the grounds that this interrogatory is vague because the term "types of information" is ambiguous.

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.

Objection: Hannaford objects to this interrogatory as burdensome and irrelevant because Hannaford is not a consumer reporting agency within the meaning of the FCRA.

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.

Objection: Hannaford objects to this interrogatory as ambiguous because the term "material factual statement or assertion" is vague. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Hannaford objects because this is a litigation interrogatory and not an investigation interrogatory, but the purported scope of the FTC's authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Hannaford objects to this interrogatory as unduly burdensome because it requires Hannaford to analyze a voluminous amount of information and insofar as it seeks information to not in the possession, custody, or control of Hannaford.

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.

Objection: Hannaford objects to this interrogatory to the extent it seeks information over which Hannaford does not have possession, custody, or control. It also objects to the interrogatory as vague because the term "harms and injuries" is ambiguous. Hannaford also objects to this interrogatory as burdensome. Finally, it objects to the interrogatory on the grounds that it lacks foundation and assumes facts not in evidence.

B. 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.

Objection: Hannaford objects to this document specification as overbroad and unduly burdensome. Hannaford also objects to this document specification because it seeks the production of documents subject to the attorney-client privilege and/or the work product privilege.

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.

Objection: Hannaford objects to this document specification as ambiguous because the term "sufficient to identify" is vague. Hannaford also objects to this document specification because it seeks the production of documents subject to the attorney-client privilege and/or the work product privilege.

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.

Objection: Hannaford objects to this document specification as overbroad, unduly burdensome, and ambiguous. It also objects to this document specification to the extent it seeks the production of documents subject to the attorney-client privilege and/or the work product privilege. It also objects to the document specification to the extent it seeks documents not in the possession, custody, or control of Hannaford. Hannaford further objects to this document

specification because it incorporates interrogatory 3 to which several objections have been asserted.

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.

Objection: Hannaford objects to this document specification as overbroad and burdensome. It also objects to this document specification to the extent it seeks the production of documents subject to the attorney-client privilege and/or the work product privilege. It also objects to the document specification to the extent it seeks documents not in the possession, custody, or control of 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.

Objection: Hannaford objects to this document specification as ambiguous because the term "sufficient to identify" is vague. Hannaford also objects to this document specification to the extent it seeks the production of documents subject to the attorney-client privilege and/or the work product privilege. Hannaford also objects to this document specification as overbroad as to time and because it seeks information on *all* claims, representations, and statements made by Hannaford regarding its collection, disclosure, use, and protection of personal information.

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.

Objection: Hannaford objects to this document specification as overbroad and ambiguous because the term "sufficient to identify" is vague.

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.

Objection: Hannaford objects to this document specification as burdensome and overbroad because not all computer networks used or operated by or for Hannaford, Sweetbay, and Shop 'n Save were affected by the intrusion. Hannaford also objects to this document specification as ambiguous because the term "sufficient to set forth" is vague.

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.

Objection: Hannaford objects to this document specification because Hannaford is not a consumer reporting agency within the meaning of the FCRA. It also objects on the grounds that the document specification is vague because the term "substantially different" is ambiguous.

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.

Objection: Hannaford objects to this document specification as unduly burdensome, overbroad and irrelevant because the GLBA and FRCA do not apply to Hannaford. Hannaford also objects to this interrogatory as vague because the terms "nature and extent of the program" is ambiguous.

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.

Objection: Hannaford objects to this document specification as ambiguous because the term "sufficient to identify" is vague. Hannaford also objects insofar as this document specification seeks documents not in the possession, custody, or control of Hannaford.

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

Objection: Hannaford objects to this document specification as ambiguous because the term "substantially different" is vague. Hannaford also objects to this document specification as irrelevant because the GLBA does not apply to Hannaford.

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

Objection: None.

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

Objection: Hannaford objects to this document specification as ambiguous because the term "substantially different" is vague.

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.

Objection: Hannaford objects to this document specification as unduly burdensome and overbroad because it seeks *all* blueprints and diagrams of countless components in its network over a five year period, *all* detailed schemes, diagrams, and blueprints of the databases containing personal information; *all* security procedures, practices, policies, and defenses, and *all* documents that concern, relate, or refer to security vulnerabilities in the network. Hannaford also objects to this document specification as ambiguous because the term "security vulnerabilities" is vague.

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

Objection: The FTC has withdrawn this document specification, pursuant to its November 23, 2010 letter. Hannaford reserves the right to assert objections to this document specification if the FTC reinstates this specification.

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.

Objection: Hannaford objects to this document specification as overbroad and unduly burdensome. It also objects to this document specification as ambiguous because the term "pharmacy information" is vague. To the extent that the FTC is attempting to use the FCRA's provision concerning medical information as a basis to seek this information, Hannaford reiterates its objection that it is not a consumer reporting agency covered by that statute. Hannaford further objects to the interrogatory as irrelevant because there was no compromise of pharmacy information.

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.

Objection: Hannaford objects to this document specification as overbroad and unduly burdensome. It also objects to this document specification as irrelevant because Hannaford is not a consumer reporting agency within the meaning of the FCRA. Hannaford also objects to the document specification as vague because the terms "sufficient to identify" and "substantially different" are ambiguous.

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.

Objection: Hannaford objects to this document specification as irrelevant because Hannaford is not a consumer reporting agency within the meaning of the FCRA.

KASH N' KARRY FOOD STORES, INC.'S OBJECTIONS TO THE FEDERAL TRADE COMMISSION'S FIRST CIVIL INVESTIGATIVE DEMAND[1]

Pursuant to 15 U.S.C. § 57b-1(b)(13), Kash n' Karry Food Stores, Inc. d/b/a Sweetbay Supermarket ("Sweetbay"), by and through its undersigned counsel, provides its objections to the first Civil Investigative Demand ("CID") of the Federal Trade Commission dated November 2, 2010 and served on November 8, 2010.

General Objections

1. Sweetbay objects to the CID as overbroad and unduly burdensome.

2. Sweetbay objects to the CID to the extent that it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, the common interest privilege, the self-evaluative privilege, or any other applicable privilege or immunity.

3. Sweetbay objects to the CID to the extent that it seeks the disclosure of information or production of documents that are confidential.

4. Sweetbay objects to the CID to the extent it seeks information or documents beyond the scope of, or seeks to impose obligations on Sweetbay beyond those authorized by, the Resolutions attached to the CID.

5. Sweetbay objects on the grounds that the Resolution attached to the CID Directing the 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 ("GLBA") and/or Section 5 of the FTC Act (File No. 002-3284) is not

[1] By letters dated November 23, 2010 and December 10, 2010, the FTC agreed to narrow certain aspects of this CID. These objections are based on the CID as narrowed by these letters. Sweetbay reserves the right to revise these objections if the FTC determines not to narrow the CID as set forth in its letters.

specifically related to the FTC's investigation of Hannaford and is not sufficient to authorize this CID.

6. Sweetbay objects on the grounds that the Resolution attached to the CID Directing Use of Compulsory Process in a 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. sec.* and/or 15 U.S.C. § 45 (File No. 992-3120) is not specifically related to the FTC's investigation of Hannaford and is not sufficient to authorize this CID.

7. Sweetbay objects to the CID to the extent it seeks information or documents over which Sweetbay does not have possession, custody, or control.

8. Sweetbay objects to the CID to the extent it seeks information or documents the disclosure of which violates consumer or employee privacy rights.

9. Sweetbay objects to the CID to the extent it seeks the disclosure of information or documents that contain health information protected under the Health Insurance Portability and Accountability Act ("HIPAA") pursuant to 42 U.S.C. § 201 *et. seq.*, 45 C.F.R. § 164.530(i), and 45 C.F.R. §§ 164.316(a).

10. Sweetbay objects to the CID insofar as it includes "contention" interrogatories, which are premature at the investigative stage and are appropriate only after discovery in litigation.

11. The following specific objections fully incorporate, are subject to, and are made without waiver of the foregoing general objections.

Objections to Definitions

1. Sweetbay objects to Definition H of "Electronically Stored Information" or "ESI" as unduly burdensome insofar as it requires Sweetbay to collect and recover, restore, or produce ESI that exists on backup media or in other forms that are not reasonably accessible.

2. Sweetbay objects to Definition K of "Hannaford" as ambiguous because the term "agents" is vague and could be read to seek information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity

3. Sweetbay objects to Definition O of "personal information" as overbroad and irrelevant because it includes information about employees, not just consumers.

4. Sweetbay objects to Definition T of "security practice" as overbroad because it defines the term to include more than technological and computer network security, and can be read to encompass door locks, facility cameras, and other non-technological or non-computer-related security.

5. Sweetbay objects to Definition V of "Sweetbay" or the "Company" as ambiguous because the term "agents" is vague and could be read to seek information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity.

Objections to Instructions

1. Sweetbay objects to Instruction D of the CID as unduly burdensome because it requires Sweetbay to catalogue and provide a voluminous amount of information in its privilege log and because the time frame provided for preparing and producing a privilege log is too short.

2. Sweetbay objects to Instruction E of the CID as overbroad and unduly burdensome because the term "in any way relevant" can be read to apply to an unmanageable volume of documents or to documents that do not contain unique, relevant information. Sweetbay further objects to this instruction to the extent it differs from, or seeks to enlarge, Sweetbay's preservation obligations beyond those provided under the applicable federal law.

3. Sweetbay objects to Instruction I of the CID to the extent it seeks the disclosure of information or production of documents subject to the attorney-client privilege and/or the work product privilege, the common interest privilege, the self-evaluative privilege, or other applicable privileges and immunities.

4. Sweetbay objects to Instruction K of the CID as unduly burdensome because it requires Sweetbay to identify for each document which specification(s) or subspecification(s) to which it responds.

5. Sweetbay objects to Instruction L of the CID on the grounds that it instructs that producing a copy of a responsive document constitutes a waiver of any claim as to the authenticity of the document.

6. Sweetbay objects to Instruction M.2 of the CID because it is ambiguous as to the format for production.

7. Sweetbay objects to Instruction M.4 of the CID as unduly burdensome because it appears that the BEGDOC field for emails is supposed to contain the same data as the BATESFIRST field for native files, making production more burdensome than if these fields had uniform names.

8. Sweetbay objects to Instruction M.4 of the CID as vague and unduly burdensome because it appears that the field PATH asks for the location where an email attachment was stored, before it was attached to the email. Sweetbay does not have that information.

9. Sweetbay objects to Instruction N of the CID because it appears to contemplate the production of personal health information that is protected by HIPAA.

10. Sweetbay objects to Instruction O of the CID as unduly burdensome because it requires to Sweetbay to identify for each piece of information the specification(s) or subspecification(s) to which it responds.

Objections to 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.

Objections: Sweetbay objects to this interrogatory as vague because the term "complete legal name" is ambiguous.

2. Identity 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, describe in detail the nature of its relationship to Sweetbay.

Objections: Sweetbay objects to this interrogatory as overbroad and seeking irrelevant information. Sweetbay further objects because Sweetbay's parent corporation is not implicated

in the investigation, is a foreign corporation outside of the FTC's jurisdiction, and is not a party to these proceedings.

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.

Objection: Sweetbay objects to this interrogatory as vague because the terms "complete legal name" and "nature of its relationship" are ambiguous. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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").

Objection: Sweetbay objects to this interrogatory as vague because the terms "each type of pharmacy information" and "receives, processes, or completes a transaction in a pharmacy located in a Sweetbay store" are ambiguous. Sweetbay also objects to this interrogatory as unduly burdensome. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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

   (a) 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 headquarters 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.

Objections: Sweetbay objects to this interrogatory as overly burdensome because it seeks voluminous information about multiple computers. Sweetbay also objects on the grounds that

the interrogatory is vague because the terms "pharmacy information" and "average weekly volume" are ambiguous. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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 it 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.

Objections: Sweetbay objects to this interrogatory as overly burdensome because it seeks voluminous information about multiple networks. Sweetbay also objects on the grounds that the interrogatory is vague because the terms "pharmacy information," "other business functions," and "whether it changed any of its back-up procedures" are ambiguous. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy 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.

Objections: Sweetbay objects to this interrogatory as overly burdensome because it seeks voluminous information about multiple networks and computers. Sweetbay also objects on the grounds that the interrogatory is vague because the terms "HIPAA computers," "security practices," "material change or update," and "extent of supervision by Sweetbay" are ambiguous. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

8. Identify and describe in detail 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.

Objections: Sweetbay objects to this interrogatory as overly burdensome because it seeks voluminous information about multiple networks. Sweetbay also objects on the grounds that the interrogatory is vague because the terms "nature of the breach," "pharmacy information," "security practices," "in response to the breach," "other types of personal information," and "material change or update" are ambiguous. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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.

Objections: Sweetbay objects to this interrogatory as vague because the term "material factual statement" is ambiguous. Sweetbay further objects to this interrogatory insofar as it seeks the disclosure of information subject to the attorney-client privilege and/or the work product privilege. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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.

Objection: Sweetbay objects to this interrogatory as burdensome. Sweetbay further objects to this interrogatory on the grounds that it lacks foundation and assumes facts not in evidence. Sweetbay also objects to this interrogatory as vague because the terms "harms and injuries" and "costs of doing so" are ambiguous. Finally, Sweetbay objects to this interrogatory to the extent it seeks information over which Sweetbay does not have possession, custody, or control. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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").

Objection: Sweetbay objects to this interrogatory as vague because the terms "material change," and "other types of personal information" are ambiguous. Sweetbay further objects to this interrogatory as overbroad because the term "security practice" is defined to include more than technological and computer network security. Sweetbay further objects on the grounds that the interrogatory is unduly burdensome because it would require Sweetbay to analyze a voluminous amount of information. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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;

    (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.

Objection: Sweetbay objects to this interrogatory as overbroad and unduly burdensome because it seeks information on *all* individuals and entities described. Sweetbay also objects on the grounds that the interrogatory is ambiguous because the terms "information security," "security practice," "the means by which Sweetbay evaluated each responsible person's performance," and "adverse actions" are vague. Sweetbay further objects to this interrogatory as overbroad because the term "security practice" is defined to include more than technological and computer network security. Sweetbay further objects on the grounds that the interrogatory is unduly burdensome because it would require Sweetbay to analyze a voluminous amount of information. Sweetbay also objects to this interrogatory as overbroad because it seeks information not in the possession, custody, or control of Sweetbay. Finally, Sweetbay also objects to the interrogatory to the extent that it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome because it would require Sweetbay to analyze a voluminous amount of information. Sweetbay also objects to the interrogatory as vague because the terms "security practice," and "goal" are ambiguous. Sweetbay also objects on the grounds that it incorporates interrogatory 11, which is also vague and unduly burdensome, as set forth above. Sweetbay further objects to this interrogatory because it seeks information not in the possession, custody, or control of Sweetbay.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome because it will require Sweetbay to analyze a voluminous amount of information given the normal personnel changes Sweetbay has experienced over the period of time covered by this CID. It further objects to the

interrogatory because it seeks information not in the possession, custody, or control of Sweetbay. Finally, Sweetbay also objects to this interrogatory as vague because it incorporates Interrogatory Specification 12, which is overbroad, unduly burdensome, vague, and insofar as it seeks the disclosure of information or production of documents subject to the attorney-client privilege, the work product privilege, or any other applicable privilege or immunity, as set forth above.

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.

Objection: Sweetbay objects to this interrogatory as duplicative of interrogatory 5 of the First/ White Paper CID the FTC issued to Hannaford. Sweetbay also objects on the grounds that the interrogatory is unduly burdensome because it seeks information for every change that is logged. It further objects to the interrogatory as ambiguous because the terms "SQL servers and applications," "extent of the use," "default password," and "other security measures" are vague. It also objects to the interrogatory as overbroad because the interrogatory seeks information about the use of default passwords on "SQL servers" on the computer networks of Sweetbay when not all servers on their computer networks were implicated in the intrusion. Sweetbay further objects to the interrogatory as irrelevant insofar as it seeks information related to pharmacy information because there was no compromise of pharmacy information.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome and overbroad. It further objects to the interrogatory as ambiguous because the terms "SQL servers and applications," "default password," "other security measures" are vague.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome and overbroad. It further objects to the interrogatory as ambiguous because the terms "administrative or other computer network account," and "the account's configuration" are vague. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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.

Objection: Sweetbay objects to this interrogatory as ambiguous overall and specifically because the term "could connect directly to the internet" is vague.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome. It also objects to this interrogatory as ambiguous because the terms "marketing or promotional activity" and

"effectiveness in achieving its purpose" are vague. It further objects on the basis that reference to "marketing or promotional activity" in this context is a mischaracterization and argumentative.

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: (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 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.

Objection: Sweetbay objects to the interrogatory as duplicative of interrogatory 8 in the First/White Paper CID to Hannaford. It also objects to this interrogatory as unduly burdensome. Sweetbay also objects to the interrogatory as ambiguous overall, and specifically because the term "churn rate" is vague, what it means for a customer to change his or her purchasing practices is vague, and because the term "demographic characteristics" is vague. It further objects to the interrogatory on the basis that it is speculative. Sweetbay also objects to the interrogatory as overbroad and seeking irrelevant information because whether or how customers may have "changed their purchasing practices" after March 17, 2008 may have nothing to do with the intrusion, particularly because the intrusion occurred in the midst of a recession and

because some of the information, such as the demographics of certain customers who pay with cash, is not within Sweetbay's control.

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.

Objection: Sweetbay objects to this interrogatory as duplicative of interrogatory 15 of the First/White Paper CID the FTC issued to Hannaford. Sweetbay also objects to this interrogatory as unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Sweetbay objects because this is a litigation interrogatory and not an investigation interrogatory, but the scope of the FTC's purported authority under the Resolutions attached to the CIDs is solely investigative. Sweetbay also objects to this interrogatory as irrelevant because there was no compromise of pharmacy information.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome because it seeks information on *all* facts, witnesses, and documents on this issue. Sweetbay also objects on the grounds that the interrogatory is vague because the term "warning of anomalous or unauthorized network activity" is ambiguous. It also objects on the grounds that this "contention" interrogatory is premature and is appropriate only after discovery in litigation. Further, Sweetbay objects because this is a litigation interrogatory and not an investigation interrogatory, but the scope of the FTC's purported authority under the Resolutions attached to the CIDs is solely investigative.

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.

Objection: Sweetbay objects to this interrogatory as unduly burdensome and overbroad.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome because it seeks a voluminous number of documents. It also objects to this document specification as overbroad because it seeks *all* documents on this issue. Sweetbay also objects on the grounds that the document specification is vague because the terms "security vulnerabilities," "gap analysis," "other security measures," "other records relating or referring to the breach," and "attackers" are ambiguous. Sweetbay also objects to the extent the document specification seeks the production of documents subject to the attorney-client privilege and/or the work product privilege.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome because it seeks voluminous documents about multiple components that make up the identified networks. Sweetbay also objects on the grounds that the document specification is vague because the terms "security practices," "documents sufficient to set forth the complete transmission or flow path for Sweetbay pharmacy information," "security vulnerabilities," are ambiguous. Sweetbay also objects to the extent the document specification seeks the production of documents subject to the attorney-client privilege and/or the work product privilege. Sweetbay also objects to this document specification as irrelevant because there was no compromise of pharmacy information.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome and overbroad because it seeks a voluminous amount of documents and seeks *all* communications. Sweetbay also objects on the grounds that the document specification is vague because the term "security products and services" is ambiguous.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome. It also objects on the grounds that the document specification is ambiguous because the terms "sufficient to identify" and "time line followed" are vague and because the entity referenced in the phrase "for each entity" is vague.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome and overbroad. It also objects on the grounds that the document specification is ambiguous because the term "substantially different" is vague.

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 o[r] for 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 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; 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;

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

(c) 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);

(d) 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

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

Objection: Sweetbay objects to this document specification as unduly burdensome because it seeks an enormous number of documents. It also objects on the grounds that the document specification is ambiguous because the terms "default password," "SQL servers and applications," "sufficient to identify," and "security measures" are vague. It also objects to the document specification as overbroad because the specification seeks documents about the use of default passwords on "SQL servers" on the computer networks of Sweetbay when not all servers on their computer networks were implicated in the intrusion. Sweetbay also objects to this document specification as unduly burdensome and overbroad because it seeks *all* communications on certain issues between Sweetbay and certain vendors, service providers, acquiring banks, card associations, and the Payment Card Industry Data Security Council, and within Sweetbay or between Sweetbay and any other person or entity regarding the use of system administrator passwords.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome. It further objects to the document specification as ambiguous because the terms "SQL servers and applications," "sufficient to identify," and "other security measures" are vague. It also objects to this document specification as overbroad because it seeks *all* documents and communications.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome and overbroad in seeking *all* documents that relate to this issue and in seeking documents on *all* functions in subspecification (a). It further objects to this document specification as ambiguous because the terms "administrative or other computer network account," and "the account's configuration" are vague.

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.

Objection: Sweetbay objects to this document specification as unduly burdensome and overbroad in seeking *all* documents. It further objects to this document specification as ambiguous because the term "security practices" is vague.

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.

Objection: Sweetbay objects to this document specification as vague because the meaning of the phrase "representative of the types, and format, of pharmacy information" is ambiguous. Sweetbay also objects on the grounds that this document specification seeks the production of personal health information that is protected by HIPAA. Sweetbay also objects to this document specification as irrelevant because there was no compromise of pharmacy information.

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

Objection: Sweetbay objects to this document specification as seeking the production of documents over which Sweetbay does not have possession, custody, or control.

12. For the period March 17, 2007 through March 17, 2009, provide all documents that describe, evaluate, or analyze changes in the purchasing practices of Sweetbay's customers, including 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 provide the underlying data, analytical methodology, and conclusions.

Objection: Sweetbay objects to this document specification as overbroad and unduly burdensome because it seeks *all* documents on the issue, which could include such documents as marketing studies about changes in peak shopping times or changes in the most popular breakfast

cereals. It also objects to the document specification as ambiguous overall, and specifically because the terms "churn rate" and "demographic characteristics" are vague.

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

Objection: The FTC has withdrawn this document specification, pursuant to its November 23, 2010 letter. Sweetbay reserves the right to assert objections to this document specification if the FTC reinstates this specification.

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

Objection: Sweetbay objects to this document specification as unduly burdensome and as seeking information beyond the scope of the Resolutions attached to the CID. Sweetbay also incorporates each of its objections to all the foregoing interrogatories to this document specification.