EXHIBIT 3

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

FAX COVER SHEET

To:	Emily Dickinson, Esq Hannaford Bros. Co.
Fax Number:	207.883.7555
No. of Pages:	11 (including cover)
Date:	March 21, 2008
Time:	3:19 pm
From:	Alain Sheer Attorney Division of Privacy and Identity Protection Bureau of Consumer Protection
Voice:	(202) 326-3321
Fax:	(202) 326-3768
E-Mail:	asheer@ftc.gov

Notes:

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Alain Sheer
Senior Attorney
Division of Privacy and Identity Protection

Direct Dial: 202.326.3321
Fax: 202.326.3629
E-mail: asheer@ftc.gov

March 21, 2008

VIA FACSIMILE AND FEDERAL EXPRESS

Mr. Ronald C. Hodge
President and Chief Executive Officer
Hannaford Bros. Co.
145 Pleasant Hill Road
Scarborough, ME 04074

Dear Mr. Hodge:

The staff of the Federal Trade Commission ("Commission") is conducting a non-public inquiry into certain information security practices of Hannaford Bros. Co. ("Hannaford"). According to recent news reports and statements issued by Hannaford, sensitive personal information (including credit card information) of customers of Hannaford stores, Sweetbay Supermarket stores, and independently-owned retail stores carrying Hannaford products was obtained without authorization from Hannaford's computer networks (hereinafter, the "breach").[1] Section 5 of the Federal Trade Commission Act prohibits deceptive or unfair acts or practices, including misrepresentations about security and unfair security practices that cause substantial injury to consumers.[2] Accordingly, we seek to determine whether Hannaford's handling of customer information raises any issues under Section 5.

As part of this review, we request that you respond to the following questions and

---

[1] *See, e.g.*, wbztv.com, *Hannaford Bros. Supermarkets Hit By Big Data Breach* (March 17, 2008), http://wbztv.com/local/retail.data.breach.2.678784.html; Hannaford Bros. Co., *Credit Card Security* (March 18, 2008), http://www.hannaford.com/Contents/News_Events/News.shtml.

[2] 15 U.S.C. § 45 *et seq.*

requests for documents by April 28, 2008. Please feel free to submit any additional information you believe would be helpful to the Commission's understanding of this matter. Any materials you submit in response to this request, and any additional information that you mark "Confidential," will be given confidential treatment.[3] In preparing your response:

- Please provide all responsive documents in the possession, custody, or control of Hannaford Bros. Co., and its parents, subsidiaries, divisions, affiliates, branches, joint ventures, and agents (hereinafter "Hannaford," "you," or "your").

- Please submit complete copies of all documents requested, even if you deem only part of a document to be responsive.

- Please number each page of your response by Bates stamp or otherwise, and itemize your response according to the numbered paragraphs in this letter.

- If any document is undated, please indicate in your response the stamped page numbers of the document and the date on which it was prepared or received by Hannaford.

- If you do not have documents that are responsive to a particular request, please submit a written statement in response. If a document provides only a partial response, please submit a written statement which, together with the document, provides a complete response.

- If you decide to withhold responsive material for any reason, including an applicable privilege or judicial order, please notify us before the date set for responding to this request and submit a list of the items withheld and the reasons for withholding each.

- Please note that we do not wish to receive documents that contain any individual consumer's date of birth, Social Security number, driver's license or other personal identification number, or financial account information. If you have responsive documents that include such information, please redact the information before providing the documents.

- We may seek additional information from you at a later time. Accordingly, you must retain all relevant records, documents, and materials (not only the information requested below, but also any other information that concerns, reflects, relates to this matter, including files and information stored electronically, whether on computers, computer disks and tapes, or otherwise)

---

[3] The Commission's procedures concerning public disclosure and confidential treatment can be found at 15 U.S.C. §§ 46(f) and 57b-2, and at Commission Rules 4.10-4.11 (16 C.F.R. §§ 4.10-4.11).

until the final disposition of this inquiry or until the Commission determines that retention is no longer necessary.[4] This request is not subject to the Paperwork Reduction Act of 1980, 44 U.S.C. § 3512.

- A responsible corporate officer or manager of Hannaford shall sign the responses and certify that the documents produced and responses given are complete and accurate.

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

REQUESTS FOR DOCUMENTS AND INFORMATION

Please provide the documents and information requested below.[5] Unless otherwise indicated, the time period covered by these requests is from January 1, 2007 through the date of full and complete production of the documents and information requested.

---

[4] Failure to retain documents that may be relevant to this matter may result in civil or criminal liability. 15 U.S.C. § 50.

[5] For purposes of this letter: the word "any" shall be construed to include the word "all," and the word "all" shall be construed to include the word "any;" the word "or" shall be construed to include the word "and," and the word "and" shall be construed to include the word "or; "the word "each" shall be construed to include the word "every," and the word "every" shall be construed to include the word "each;" and the term "document" means any preexisting written or pictorial material of any kind, regardless of the medium in which such material was created, and regardless of the method by which it is stored (*e.g.*, computer file, computer disk or tape, microfiche, etc.).

General Information

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

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

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

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

   (a) identify the type(s) of personal information stored and processed on the network, the source of the 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:

   (1) 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);

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

(3) 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) provide documents setting out, and describe in detail, the security procedures, practices, policies, and defense(s) (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;

(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; and

(e) provide the name(s), title(s), and contact information of the individual(s) responsible for creating, designing, managing, securing, and updating the network.

The responses to each subpart of this Request should describe in detail each material change or update 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 reason(s) for the change or update.

Information About The Breach

5. Public statements issued by Hannaford have reported that an intrusion into its computer networks compromised credit and debit card information obtained from customers. *See, e.g.*, Hannaford Bros. Co., *Credit Card Security* (March 18, 2008), http://www.hannaford.com/Contents/ News_ Events/News.shtml ("Hannaford has contained a data intrusion into its computer networks that resulted in the theft of customer credit and debit card numbers."). Describe in detail, and produce documents that identify, how and when Hannaford first learned about the breach.

6. Describe in detail, and provide documents setting out, the process(es) 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 Request 6(a), above, 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 computer(s) or server(s) used to aggregate authorization requests from individual stores and transmit them to bank associations and banks ("card authorization server"), and, for each server, identify the application(s) 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.

7. 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 type(s) and amount(s) of information that was 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 attacker(s).

8. 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 Request 3, above, 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.

9. According to a Wall Street Journal article, Hannaford "knows of about 1,800 cases of fraud stemming from the breach." Joseph Pereira, *Chains Report Stolen Card Data*, Wall Street Journal (March 18, 2008), http://online.wsj.com/article_print/SB120578480456942847.html. 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 bank(s) 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's 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.

10. 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.

11. 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. If notification has been made, explain why notification was made (*e.g.*, compelled by law) 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.

12. According to Digital Transaction News, Hannaford "had recently upgraded our wireless encryption." *Hannaford Bros. Was in Compliance with PCI When Hacked*, Digital Transaction News (March 18, 2008), http://www.digitaltransactions.net/newsstory.cfm?newsid=1712. Provide:

    (a) a detailed narrative describing the upgrades made to 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; and

    (b) 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. *See e.g.*, *Independent Store List*, Hannaford Bros. Co. (March 18, 2008), http://www.hannaford.com/Contents/News_Events/news/independent.shtml. 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 all 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.

13. In connection with the breach, Hannaford provided information to Canadian customers. Hannaford Bros. Co., *Canadian Recommended Steps* (March 18, 2008), http://www.hannaford.com/Contents/News_Events/News/Canada

Customer.shtml. Provide:

(a) documents sufficient to identify, and describe in detail: all networks located outside of the United States used by Hannaford to store and process personal information; the physical location(s) of each network; and the function(s) and business purpose(s) of each network;

(b) blueprints and diagrams setting out in detail the components, topology, and architecture of each network identified in the response to Request 13(a), above;

(c) for each system identified in response to Request 13(a), above, describe in detail the extent and nature of any interconnection or interface with Hannaford networks located in the United States; and

(d) documents sufficient to identify: the number of Canadian customers whose information was or may have been obtained through the breach; the types and amounts of information that was or may have been obtained; and the country where the information was originally collected.

Other Information

14. 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 date(s) when it was adopted or made, to whom it was distributed, and all means by which it was distributed.

15. 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.

Please send all documents and information to: Alain Sheer and Molly Crawford, Division of Privacy and Identity Protection, Federal Trade Commission, 600 Pennsylvania Ave., NW, Mail Stop NJ-3137, Washington, D.C. 20580. Due to extensive delays resulting from security measures taken to ensure the safety of items sent via the U.S. Postal Service, we would appreciate receiving these materials via Federal Express or a similar delivery service provider, if possible.

Thank you for your prompt attention to this matter. Please contact me (at 202.326.3321) or Molly Crawford (at 202.326.3076) if you have any questions about this request or need any

additional information.[6]

Sincerely,

Alain Sheer
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission Division

[6] The Commission has a longstanding commitment to a fair regulatory enforcement environment. If you are a small business (under Small Business Administration standards), you have a right to contact the Small Business Administration's National Ombudsman at 1-888-REGFAIR (1-888-734-3247) or www.sba.gov/ombudsman regarding the fairness of the compliance and enforcement activities of the agency. You should understand, however, that the National Ombudsman cannot change, stop, or delay a federal agency enforcement action. The Commission strictly forbids retaliatory acts by its employees, and you will not be penalized for expressing a concern about these activities.

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

FAX COVER SHEET

To: Daniel F. McInnis, Esq

Fax Number: 202.887.4288

No. of Pages: 6 (including cover)

Date: July 23, 2008

Time: 10:30AM

From: Alain Sheer
Attorney
Division of Privacy and Identity Protection
Bureau of Consumer Protection

Voice: (202) 326-3321
Fax: (202) 326-3768
E-Mail: asheer@ftc.gov

Notes: As discussed yesterday.

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Alain Sheer
Attorney
Division of Privacy and Identity Protection

Direct Dial: 202.326.3321
Fax: 202.326.3629
E-mail: asheer@ftc.gov

July 23, 2008

VIA FACSIMILE AND FEDERAL EXPRESS

Daniel F. McInnis, Esq.
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Ave. NW
Washington, D.C. 20036-1564

Dear Mr. McInnis:

Thank you for providing us with documents and information about the recent breach at Hannaford Bros. Inc. ("Hannaford") as well as the company's information security practices generally. As we discussed yesterday, we have reviewed materials submitted in response to our March 21, 2008 access letter, and have some follow-up questions. All instructions and definitions from our March 21, 2008 letter apply to this request, and we have continued the numbering from that letter. As we mentioned yesterday, we would like to meet on August 11, 2008 and ask that you provide the following information by August 8, 2008:

16. According to Hannaford's responses to Requests 2 and 3, it provides services related to processing electronic payment transactions for independently-owned stores ("collectively, "Shop n' Save") and Sweetbay stores (collectively, "Sweetbay"). Please identify each such service, including, but not limited to: authorization services through which Hannaford receives credit, debit, and EBT card authorization requests from Shop n' Save or Sweetbay stores, 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 stores use in conjunction with a service; providing sales data for transactions processed at Shop n' Save or Sweetbay stores; providing network services; providing settlement services; or providing transaction history information.

17. For each service identified in the response to Request 16:

    (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, and each

store operated by any other entity, to which Hannaford provides the service (collectively, "recipient entities");

(c) 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 and recipient entities, 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;

(d) provide copies of all substantially different documents that set out the terms and conditions under which Hannaford provides the service to recipient entities, including, but not limited to, contracts to supply the service as well as hardware, software, or technical support used in providing the service. If there are no responsive documents, please describe the terms and conditions in detail; and

(e) identify the annual revenue or cost saving (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 stores, Sweetbay stores, and stores operated by other entities.

18. According to Hannaford's response to Request 5(a), it issues a private "Service Plus" payment card to both individual and institutional customers and is responsible for transmitting, processing, and authorizing all payments made with the Service Plus card. 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 process(es) by which individuals and institutions are approved to participate in the program; the service(s) provided by and/or benefit(s) obtained through the program (such as advancing credit for purchases); the type(s) and amount(s) 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.

19. Hannaford's May 16, 2008 narrative response briefly describes a payroll check cashing program. For this program, please: identify the annual number of payroll checks Hannaford has cashed over the period set out in the access letter; the number of customers for whom Hannaford has cashed payroll checks; the nature of the relationship between Hannaford and customers presenting payroll checks to be cashed (for example,

retail customers); and the application or other process followed to enroll customers in the program, including the information customers must provide to enroll in the program.

20. According to Hannaford documents, prescription transactions were compromised during the breach (*see* HAN-E-0045452). Please: identify the types of information contained in the prescription transactions that were compromised as well as the stores where the transactions were compromised; provide all documents relating to whether pharmacy information was accessed without authorization, including, but not limited to, audits or assessments; and, for each store where pharmacy transactions were compromised, describe the nature of the breach. Further:

(a) identify 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) for each pharmacy network:

(1) identify the type(s) of pharmacy information stored and processed on the network and the source of each type of information;

(2) provide 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);

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

(4) provide documents setting out, and describe in detail, the security procedures, practices, policies, and defense(s) (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

(5) provide 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;

(c) provide all 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;

(d) provide the name(s), title(s), and contact information of the individual(s) responsible for creating, designing, managing, securing, and updating the pharmacy networks; and

(e) identify 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.

The responses to each subpart of this request should describe in detail each material change or update 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 reason(s) for the change or update.

21. Provide a detailed explanation of document HAN-E-16264 (which states that the back-up process for pharmacy data was changed in March 2008 to the POS server which is now encrypted), including, but not limited to: an explanation of how pharmacy data was backed-up before March 2008; the types of pharmacy data and other information held on the POS server and period of time for which such information was held; whether pharmacy data was encrypted before the March 2008 change; why the back-up process was changed; and the location of the POS server within Hannaford's networks.

22. Hannaford's responses to our access letter included several Payment Card Industry Data Security Standard ("PCI") assessments conducted by Verisign and CyberTrust.

(a) with respect to the Verisign assessment, Hannaford's response to Request 7 states that "Hannaford takes the position that this PCI Incident Report includes many factual statements and assertions that are inaccurate and not germane to the cause and effect of the data intrusion." Please identify each material factual statement or assertion you dispute, and explain in detail the basis for your position; and

(b) with respect to the PCI assessment performed by CyberTrust in January and

February 2008, please:

(1) 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; and

(2) unless the assessment sample included the entire PCI system, identify which networks and components were not included in the sample, explain why these networks and components were not included, and identify who decided to exclude them.

Thank you for your prompt attention to this matter. Please contact me (at 202.326.3321) or Ellen Ginsberg (at 202.326.3787) if you have any questions about this request or need any additional information.

Sincerely,

Alain Sheer
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission Division

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Alain Sheer
Senior Attorney
Division of Privacy and Identity Protection

Direct Dial: 202.326.3321
Fax: 202.326.3629
E-mail: asheer@ftc.gov

BY EMAIL

Michael Oakes, Esq.
Hunton & Williams LLP
1900 K Street NW
Washington, DC 20006

September 8, 2009

Dear Mike:

As we discussed last Friday, there are several types of information we do not have and would like to see as part of the Hannaford investigation. We have searched the company's submissions for these materials without success, but if they are in the submissions, please let me know the Bates numbers. Following the instructions set out in our access letters, please provide:

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

2. updated information about claimed harms and injuries resulting from the breach, including, but not limited to, documents and a narrative setting out:

(a) the number of payment cards of all kinds (such as credit, debit, EBT, and insurance cards) that were or may have been compromised;

(b) the number of cards that have been used to make fraudulent purchases and the dollar value of the fraudulent purchases;

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

(e) the number of checking or other bank accounts that were closed and reopened at a different institution or under a different account number, and all costs incurred in doing so; and

(f) copies of documents settling claims and/or reimbursing claims for costs related to the breach.

3. a copy of each substantially different contract with Catalina.

4. information that concerns or relates to card processing and related services Hannaford provided to the Shop n' Save and Sweetbay chains, including, but not limited to, documents and a narrative setting out:

(a) the number and dollar value of card transactions that were processed monthly (or if not recorded on a monthly basis, then as periodically recorded) for each chain;

(b) for Hannaford, the number and dollar value of card transactions for purchases in Hannaford stores that were 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 Hannafod's charge to each chain for each separate component of the services (such as for POS equipment, maintenance, interchange fees, and other payment card fees, as set forth on page 3 of the company's August 8, 2008 response to our access letters);

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

(d) 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.

Please call if you have questions, and feel free to provide other materials that you believe will be helpful.

Sincerely,

Alain Sheer
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission Division

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

Alain Sheer
Senior Attorney
Division of Privacy and Identity Protection

Direct Dial: 202.326.3321
Fax: 202.326.3629
E-mail: asheer@ftc.gov

BY EMAIL

Michael Oakes, Esq.
Hunton & Williams LLP
1900 K Street NW
Washington, DC 20006

October 14, 2009

Dear Mike:

As we discussed last week, there are several items of information that we would like to review for our meeting on October 23, 2009. The information concerns compliance with the Fair Credit Reporting Act ("FCRA") as it relates to decisions approving or declining the personal checks of customers in Hannaford, Sweetbay, and Shop n' Save stores. Following the instructions set out in our access letters, please provide:

1. documents sufficient to identify and describe in detail 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 in Hannaford, Sweetbay, or Shop n' Save stores to pay for their purchases or obtain cash. The response 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); (f) a copy of each substantially different adverse action notice that has been provided to customers; and (g) a narrative describing how adverse action notices are provided to customers whose personal checks have been declined.

2. 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 stores; and a narrative that identifies the items of information that each vendor provides and describes how Hannaford

obtains access to the information (such as by 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).

3. separately for Hannaford, Sweetbay, and Shop n' Save stores: (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.

Please call if you have questions, and feel free to provide other materials that you believe will be helpful.

Sincerely,

Alain Sheer
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission Division