



1385 Hancock Street
Quincy, MA 02169

Robert A. Licht, Vice President of Business Law
Telephone: 617-770-6231
Fax: 617-770-6980

June 23, 2006

Mr. Joshua Stein
NC Attorney General's Office
Consumer Protection Provision
9001 Mail Service Center
Raleigh, NC 27699-9001

Dear Mr. Stein:

We are writing to inform you of a data security breach involving individuals' personal information pursuant to the requirements of NCGS § 75-65(f).

We have been informed by one of our external vendors that a laptop computer containing Ahold USA's data pertaining to both grants and exercises of Ahold stock options in 2005 was lost from the checked baggage of a domestic commercial airline flight on April 13, 2006. The incident was immediately reported to the airline and to the police. We were first informed by our vendor of this incident on June 7, 2006.

Although we have no indication that any of the information is being misused, as a result of this incident and pursuant to requirements under North Carolina law, we are notifying you of the following concerning the timing, distribution, and content of the notice we are sending to affected individuals:

- We are preparing a notification letter for individuals whose information may have been involved in the incident (a copy of our notification letter is attached).
- We will send the notification letter to individuals whose information may have been involved in the incident – we estimate that approximately 3,500 individuals nationwide will receive notification. We expect that the notification letters will be mailed commencing June 23, 2006.
- We are notifying all three consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in 15 U.S.C. § 1681a(p)) of the breach. Our notification to these agencies will provide information relating to the timing, distribution, and content of the notice that will be sent to individuals, including a copy of the notification letter.

We are available to answer any questions you may have regarding this incident and our notification to our customers.

Very truly yours,



Robert A. Licht

Vice President of Business Law

RAL/mff
Enclosures

Name

Street Address

City, State, Zip Code

Dear []:

We are writing to let you know about an unfortunate incident that may have exposed your personal information to others. While we have had no indication that your information is being misused, we wanted to report the incident to you and inform you of steps you can take to protect yourself from possible identity theft.

We have been informed by Deloitte Accountants, our external auditing firm, that an employee of Deloitte Tax had her laptop computer stolen from baggage checked on an April 13 domestic commercial airline flight. The incident was immediately reported to the airline and to the police. In the course of its incident response investigation, Deloitte first determined on June 1 that a file with your personal information was most likely on the laptop. Deloitte informed us of the situation the following week. As soon as we were notified by Deloitte we assembled a team to review and verify the facts and circumstances of this incident and develop a response. As of this time, the laptop has not been located.

The file was being used by Deloitte to test certain 2005 Ahold stock option activity in connection with the audit of Ahold's 2005 financial statements. It included your name, Social Security Number, date of birth for persons who received Ahold option grants in 2005, and information related to both grants and exercises of Ahold stock options in 2005. No financial account or medical benefits information was in the file. The laptop was protected by an identity verification process that incorporated a unique user ID and a password, but the file itself was not additionally password protected or encrypted. Deloitte has informed us that its employee violated the Deloitte Tax information security policy by checking the laptop in baggage on a commercial airline flight.

Because we cannot rule out the possibility of your information being misused, we have arranged for the following services to help protect you from identity theft. We recommend you use these services and follow the additional steps described in the following paragraphs. However, it is up to you to decide whether to follow these steps; neither the company nor anyone else can make that decision for you or sign you up for these services.

- A help line at toll-free **800-562-2318** has been established to assist you with questions and concerns. The help line will be staffed from 8:30 a.m. to 5:00 p.m. Eastern time, Monday through Friday, from today to September 22, 2006. You may leave a message after hours and you will receive a callback the next business day.
- You can contact one of the major U.S. credit bureaus listed below and have a "fraud alert" placed on your credit file at all three bureaus. This fraud alert lets creditors know additional steps should be taken to verify your identity prior to granting credit in your name. There will be no charge to you for this fraud alert.

Credit Bureau	Toll-Free No.	Website
Experian	888-397-3742	www.experian.com
Equifax	877-478-7625	www.equifax.com
TransUnion	800-680-7289	www.transunion.com

- You can enroll in credit monitoring for the next year, at no charge to you. Once enrolled, you will receive communications detailing any key changes to your credit report from all three credit bureaus. If there is no activity, you will be updated on a monthly basis. To enroll, contact the call center to obtain instructions and a promotional code and then register at www.myservices.equifax.com/tri. If you do not have access to the Internet, the call center can provide instructions on how to register by mail.

You are also entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free (877) 322-8228. For additional information on how to further protect yourself against identity theft, you may wish to visit the web site of the U.S. Federal Trade Commission at www.consumer.gov/idtheft/.

You may have recently heard or been notified of a separate incident which occurred involving the loss of the laptop of an Electronic Data Systems (“EDS”) employee on a commercial flight in May which contained certain personal information of retirees participating in the Ahold Pension Plan and certain other former employees of Ahold USA, Inc. or its retail supermarket subsidiaries. Please be advised that this stolen laptop incident relating to Deloitte is separate and unrelated to the EDS incident. However, if you were previously notified as a potentially affected person relating to the EDS incident and you obtained a promotional code and activated a fraud alert and credit monitoring membership, you have the proper protection in place and do not need to do it again.

The security of associates’ personal information is important to us, and we work to ensure our vendors have processes in place to keep it safe. We are very disappointed by this incident, and we regret any inconvenience or concern this may cause you.

We are taking steps to help prevent security incidents like these from happening again. While Ahold currently has in place policies and expectations concerning information security, both internally and also with our external service providers, we are undertaking a comprehensive and thorough review of such policies. We plan to evaluate and, where appropriate, implement additional safeguards both internally and also with our third party vendors.

Sincerely,

Jim Lawler
Ahold Chief Human Resources Officer



ROBERT A. LICHT
Vice President of Business Law
Ahold USA, Inc.
c/o The Stop & Shop Supermarket Company LLC
1385 Hancock Street
Quincy, MA 02169
617-770-6231
617-770-6980 - Fax

20

July 17, 2006

Kim D'Arruda, Esq.
Assistant Attorney General
Consumer Protection/Antitrust Division
State of North Carolina
Department of Justice
9001 Mail Service Center
Raleigh, NC 27699-9001

Re: Security Breach Notification

Dear Attorney D'Arruda:

I am responding to your letter of July 9, 2006 confirming receipt of my June 23, 2006 notice concerning a data security breach pertaining to individuals who received grants of and/or exercised Ahold stock options in 2005.

Approximately 96 of the persons affected by this breach are North Carolina residents. The laptop that was reported missing was in the possession of an employee of Deloitte Tax, an affiliate of Deloitte Accountants, Ahold's external auditor. The laptop was protected by a unique user identifier and a password. The data file on the laptop was not additionally password protected nor encrypted. While Deloitte immediately reported the laptop computer as stolen to the airline and to the police, it took Deloitte additional time to identify the information that was on the laptop and to inform Ahold. There was no delay attributable to the law enforcement investigation.

We are also concerned that this incident was the second one involving an outside vendor in a short period of time. However, we do not believe it is evidence of a pattern of carelessness, since both situations involved employees of our vendors who checked their laptops on a commercial airline flight in contravention of both their employer's policy as well as common sense business practice.

Once we were informed of this incident on June 7, we proceeded to work with Deloitte to put in place promptly the measures described in my letter of June 23, 2006 and the attached notice letter to the affected individuals. Those measures are designed to help reduce the possible misuse of information. Ahold is continuing its comprehensive review of our policies and practices concerning information security, and we are in the process of taking affirmative steps

to effectively communicate procedures and policies with the objective of enhancing our ability to control the security of the personal information of both our employees and customers. I enclose a copy of an internal communication broadly distributed within Ahold which is a significant step toward increasing awareness of both the importance of information security and the tools available to our associates to help safeguard both personal and company confidential information.

Please feel free to call me directly at 617-770-6231 if I can provide any additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "RAL", written over a light blue horizontal line.

Robert A. Licht

Vice President of Business Law

RAL/mff

Att: June 22, 2006 Lawler Memo

To: Distribution
From: Jim Lawler
Date: June 22, 2006
Subject: Employee Information

We've recently observed disappointing issues concerning the loss of confidential employee data by third party service providers. These instances have involved a company's handling of information provided to it by Ahold, as well as the handling of other companies' confidential information. Therefore, this message is meant to reinforce our expectations about laptop security and the handling of confidential employee information with third parties:

Disclosure of Employee Information

- Confidential employee information includes without limitation the combination of employee name and other private information such as date of birth, spouse's name, social security number, SOFI number, driver's license number, earnings data or benefits eligibility.
- Access to confidential employee information is to be limited on a need-defined basis.
- Saving data on desktops, laptops and external devices such as flash drives, memory sticks and CDs is discouraged because portable devices can be lost or stolen and locally saved data can otherwise be compromised. Accordingly, employees who have access to confidential employee information should only save such information onto their laptops, desktops or external devices when necessary. Files that are saved locally should be password protected and encrypted. If you need instructions on how to do this, please refer to the instructions at <http://protectinfo.ahold.com> or call your helpdesk. A list of helpdesk numbers is attached.
- Confidential employee information should not be provided to external parties without the authorization of a manager, and only employee information that is absolutely essential to a task should be communicated. Any ancillary information in a file that is not specifically necessary for the task being handled by the third party should be eliminated from the file.
- You should not transmit unencrypted files containing confidential employee information. As noted, for assistance in encrypting files, please refer to the instructions at <http://protectinfo.ahold.com> or call your helpdesk.
- When transmitting a file containing confidential employee information to a third party you should include a statement in the cover message that the information is confidential and must be treated in accordance with Ahold's policies regarding confidential information. In addition, the file itself should include a notice

indicating that it contains confidential information. A sample transmittal statement and confidentiality notice are as follows:

- **Transmittal Statement:** “This message (including any attachments) contains information that may be confidential to [Opco name] or its affiliates. If you are the intended recipient, you are authorized to use the information only as expressly authorized by [Opco name] and must strictly adhere to applicable security procedures, including without limitation the following:
 - You must protect files using the password and level of protection in which the file was provided to you; and
 - You may transmit files only as necessary for the task you are assigned using secure systems and appropriate encryption means.If you have received the message in error, please advise the sender by reply e-mail, and destroy all copies of the original message (including any attachments). Please direct any questions to the sender of this message.”

- **Confidentiality Notice:** “This File Contains Confidential and Proprietary Information of [Opco name].”

Laptop Computer Security and other mobile devices

Ahold associates are responsible for observing common sense precautions necessary to protect your laptop computer from loss or theft. These include, without limitation:

- *Never* check your laptop computer and other mobile devices like PDA's, Memory sticks etc. as baggage on an airline flight (this includes plane-side check for bags which will not fit in the overheads); and
- *Never* leave your laptop or other mobile devices unattended in an unsecured location.

Failure to comply with these minimum expectations may compromise the security of Ahold's business information and will result in disciplinary action up to and including termination.

I know that we all appreciate the importance of protecting confidential information, and therefore that taking the necessary precautions is something that should be considered “standard practice,” however, based on the experiences of other companies who have faced compromises of such data, we can never be too vigilant.

Thank you for your attention to this issue.

Helpdesk Numbers

Operating\Support Company	Number
Ahold Central Europe	
Czech/Slovakia	+420234004260
Poland	+48126394343
Ahold GSO	+31 20 509 5222
Albert Heijn	+31 75 659 2100
Stop & Shop/Giant-Landover	1-800-246-5334
Giant-Carlisle/Tops/Martins	1-800-246-5334 (Tops: X5555, Giant: X7640)
Peapod	1-888-492-4110
U.S. Foodservice	1-888-648-2580
AIS / AFS / PPO / ASC / MAC Risk Management / Not for Resale (Braintree)	1-800-246-5334