David A. Zetoony
Direct: (202) 508-6030
david.zetoony@bryancave.com

February 1, 2010

CONFIDENTIAL

VIA FEDERAL EXPRESS

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Data Security Breach Notification

To Whom It May Concern:

This letter is intended to notify the Office of the Maryland Attorney General that Ceridian Corporation ("Ceridian"), a client of Bryan Cave LLP, intends to notify approximately 514 residents of the State of Maryland that their personal information may have been accessed or acquired by an unauthorized individual.

Ceridian is a business services company that offers a range of business support products, including human resource solutions, payroll and payment systems, benefits administration services, and productivity and wellness products.

On December 23, 2009, Ceridian identified unusual activity that might indicate a potential data security breach. Ceridian immediately implemented a responsive action plan to investigate the unusual activity consisting of the following:

(1) Ceridian conducted an internal investigation to determine the source of the unusual activity.

(2) On December 28, 2009, Ceridian concluded that the source of the unusual activity was an unauthorized hacker.

(3) On December 29, 2009, Ceridian alerted the Federal Bureau of Investigation, which referred the matter to its Atlanta Field Office.

(4) By January 11, 2010, Ceridian was able to identify, with reasonable certainty, specific files and information that may have been illegally

Bryan Cave LLP
1155 F Street N.W.
Washington, D.C. 20004
Tel (202) 508-6000
Fax (202) 508-6200
www.bryancave.com

accessed and/or acquired. Ceridian immediately began a process to identify and reconcile the names, and residences, of those individuals.

(5) On January 28, 2010, Ceridian notified the consumer reporting agencies of the event.

(6) Beginning on or about January 29, 2010, Ceridian began notifying the Maryland residents whose personal information may have been accessed and/or acquired in connection with this event. A sample of the notification letter sent to those residents is included as Attachment A. As noted in that letter, Ceridian is offering affected Maryland residents one year of free credit file monitoring to help protect them against possible identity theft.

Ceridian remains committed to working with the Federal Bureau of Investigation and appropriate local law enforcement agencies to investigate and prosecute those responsible for this illegal conduct.

If you would like any additional information concerning the above referenced event, please feel free to contact me at your convenience.

Sincerely,

David A. Zetoony

Enclosure

Ceridian
3311 East Old Shakopee Road
HQE03C
Minneapolis, MN 55425-1640

CERIDIAN

Attachment A

January 29, 2010 **Sample Consumer Notification Letter**

[Consumer Name]
[Consumer Address]

Enrollment Code :

Dear [Consumer Name]

This letter is to notify you that some of your personal information from Ceridian's US-based Powerpay web application may have been illegally accessed by an unauthorized hacker. Ceridian's Powerpay system is used by your employer (or past employer) to prepare your payroll. In light of these events, we want you to be fully apprised of the situation, the actions we have taken, and the actions you can take to protect the continued privacy and security of this information.

Event Summary

Late last month Ceridian determined that an unknown hacker accessed our Powerpay application on December 22 and 23. Working with law enforcement and professional investigators, we were able to recreate the event and determine what the hacker was able to access. Based on our investigation, we believe that the information accessed included your first name, last name, social security number, and, in some cases, birth date and/or the bank account that is used for direct deposit of your pay. (If you receive a check rather than a direct deposit, Ceridian does not have your bank account information).

Protective Action

In light of this event, Ceridian has arranged to provide you with one-year of free credit file monitoring and identity theft protection through Equifax Credit Watch Silver™. Information on how to enroll in the program is enclosed with this letter. Whether you choose to enroll in this product or not, you can:

1. Remain vigilant for possible identity theft by reviewing and monitoring your credit report regularly. You can obtain a free annual credit report from one, or all, of the national consumer reporting agencies by visiting http://www.annualcreditreport.com, or by calling toll-free 877-322-8228. When you receive the report it should be reviewed carefully and you should notify the credit agencies of any inaccuracies or unrecognized accounts. You may also enroll, at your cost, in an identity theft monitoring or credit monitoring product or service other than the Equifax product being offered herein.

2. Take steps to prevent unauthorized access to any accounts you have with any financial institution. This includes bank accounts, credit cards, brokerage accounts, etc. You may want to contact such institutions and notify them of the information that may have been compromised and follow any steps they may suggest to safeguard access to your accounts with them. Also, you should check your periodic statements from each of the financial institutions promptly upon receiving them to be sure that no unauthorized transactions have occurred.

3. In the event that you determine that an account has been fraudulently established, or accessed using your identity, you can call the national consumer reporting agencies and your financial institutions, as well as immediately contact the Federal Trade Commission, and your state's Attorney General. Contact information for these consumer reporting agencies, the FTC and states' Attorney Generals, and certain important notices, is also enclosed with this letter. You can also call your local police or sheriff's office to file a police report or any unauthorized activity you discover. If you do so, you should obtain a copy of the police report for your records and future reference.

000001-000001

4. Additional information about reporting and preventing identity theft can be found at http://www.ftc.gov/bcp/edu/microsites/idtheft/, or from your state's Attorney General. Among other things, this website explains how to ask the national credit reporting agencies to place a "fraud alert" or "security freeze" on your credit reports. A fraud alert is a consumer statement added to your credit report that alerts creditors of possible fraudulent activity within your report. A security freeze (also known as a credit freeze) prevents credit reporting agencies from releasing your credit report without your consent. As a result, using a security or credit freeze may interfere or delay your ability to obtain credit. Further, unlike a fraud alert, you must separately place a security or credit freeze on your credit file at each credit reporting agency. In addition, you should note that placing a security or credit freeze on your credit file will prevent you from participating in the Eqiufax Credit Watch™ product.

   If at any time you feel it is necessary, you can contact the credit reporting agencies to place such a fraud alert or security or credit freeze on your credit file, including by visiting http://www.fraudalerts.equifax.com or calling Equifax's auto fraud line at 1-877-478-7625 and following the automated prompts. Additional contact information for Equifax and other major credit reporting agencies is enclosed with this letter. There may be fees for placing, lifting and/or removing a freeze and in order to request a freeze you will be required to provide the following information/items: (1) your full name, Social Security Number, and date of birth; (2) if you have moved in the past five years, the addresses where you have lived over the past five years; (3) proof of current address, such as a current utility bill or telephone bill; (4) a legible photocopy of a government issued identification card, such as a state driver's license or ID card, military identification, etc.; (5) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to law enforcement agency concerning the theft; and (6) if you are not a victim of identity theft, payment by check, money order, or credit card (do not send cash through the mail).

Other Protective Steps

If you receive your pay by direct deposit, and therefore your bank routing and account information may have been compromised, you may want to discuss this situation with your bank. Whether or not you should change your bank account as a result of this event is a decision that is different for every person depending on personal circumstances. Your bank will have the best advice for your particular situation.

000001-000001

Ceridian is committed to maintaining the privacy and security of all confidential employee data and undertakes many precautions for the security of personal information, including regular review and evaluation of the security of all processes. This unprecedented situation has our full attention and we are taking aggressive actions to guard against such events in the future.

We deeply regret this event and sincerely apologize for any concern and inconvenience it may cause you. If you have questions or need further information, please call 1-800-550-1538. This call center will be operational Monday - Friday between 9 a.m. and 9 p.m. EST until February 26, 2010.

Sincerely,

CERIDIAN CORPORATION

John F. Hunter
Executive Vice President and General Manager
US Payroll Business

CERIDIAN CORPORATION

Angela J. Carfrae
VP, Information Protection Services

How to Enroll in Equifax Credit Watch™ Silver

About Equifax Credit Watch™ Silver

Equifax Credit Watch will provide you with an "early warning system" of changes to your credit file and help you to understand the content of your Equifax credit file. The key features and benefits are listed below.

Equifax Credit Watch provides you with the following benefits:

- Comprehensive credit file monitoring of your Equifax credit report with weekly notification of key changes to your credit file.
- Wireless alerts and customizable alerts available.
- One copy of your Equifax Credit Report™.
- $25,000 in identity theft insurance with $0 deductible, at no additional cost to you. †
- A 24 hour a day, 7 day a week live agent customer service center to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and to assist you in initiating an investigation of inaccurate information.
- 90-day Fraud Alert placement with automatic renewal functionality (available online only).

How to Enroll in Equifax Credit Watch™ Silver

To sign up online for **online delivery** go to www.myservices.equifax.com/silver

1. Consumer Information: complete the form with your contact information (name, address and e-mail address) and click "Continue" button. The information is provided in a secured environment.
2. Identity Verification & Payment Code: complete the form with your Social Security Number, date of birth, telephone #s, create a User Name and Password, agree to the Terms of Use, enter the code 444444444444 in the "Enter Promotion Code" box and click "Continue." This code eliminates the need to provide a credit card number for payment. The system will ask you up to two security questions. This is the Equifax Identity Verification Process.
3. Order Summary: click "Continue" button.
4. Order Confirmation: - Click "View My Product" to access your Credit Report and other product features.

† Insurance underwritten by member companies of American International Group, Inc. The description herein is a summary only. It does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for complete details of coverage and exclusions. This product is not intended for minors (under 18 years of age).

000001-000001

000001-000001

Important Contact Information If You Believe That You May Be The Victim of Identity Theft

Consumer Reporting Agencies

Company	Telephone	Address	Website
Equifax	877-478-7625	P.O. Box 740241 Atlanta, GA 30374-0241 or P.O. Box 105788 Atlanta, GA 30348	http://www.equifax.com
Experian	888-397-3742	P.O. Box 9532 Allen, TX 75013 or P.O. Box 9554 Allen, TX 75013	http://www.experian.com
TransUnion	800-680-7289	Fraud Victim Assistance Division P.O. Box 6790 Fullerton, CA 92834-6790	http://www.transunion.com

Federal Trade Commission

Agency	Telephone	Address	Website
Federal Trade Commission	877-438-4338	Consumer Response Center 600 Pennsylvania Avenue, NW Washington, DC 20580	https://www.ftccomplaintassistant.gov/

000001-000001

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For North Carolina Residents: You can obtain information from the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact Attorney General Roy Cooper's Consumer Hotline toll-free within North Carolina at 1-877-5-NO-SCAM.

State Attorneys' General or State Consumer Protection Division

State	Contact Information
Alabama	334.242.7300 or 1.800.230.9485
Alaska	907.465.2133 or 907.269.5200
Arizona	520.628.6504 or 800.352.8431
Arkansas	501.682.2341 or 800.482.8982
California	916.322.3360
Colorado	303.866.4500
Connecticut	860.808.5318
Delaware	800.220.5424 or 302.577.8600
District of Columbia	202.724.1305
Florida	850.414.3990
Georgia	404.651.9340 or 404.656.3790
Hawaii	808.586.1500
Idaho	208.334.2424
Illinois	1.866.999.5630
Indiana	317.2326330 or 1.800.382.5516
Iowa	515.281.5926 or 888.777.4590
Kansas	785.296.3751 or 800.432.2310
Kentucky	502.696.5389 or 800.804.7556
Louisiana	225.326.6400 or 1.800.351.4889
Maine	207.626.8800 or 1.800.436.2131
Maryland	410.528.8662 or 410.576.6491
Massachusetts	617.727.8400 or 1.877.438.4338
Michigan	517.373.1110
Minnesota	651.296.3353
Mississippi	601.359.3680
Missouri	573.751.3321
Montana	406.444.2026

State	Contact Information
Nebraska	402.471.2682
Nevada	775.684.1100
New Hampshire	603.271.3658
New Jersey	609.292.8740
New Mexico	505.827.6000
New York	518.474.7330
North Carolina	919.716.6400
North Dakota	701.328.2210
Ohio	614.466.4320
Oklahoma	405.521.3921
Oregon	503.378.4732
Pennsylvania	717.787.3391
Puerto Rico	787.721.2900
Rhode Island	401.274.4400
South Carolina	803.734.3970
South Dakota	605.773.3215
Tennessee	615.741.5860 or 615.741.1671
Texas	512.463.2100
U.S. Virgin Islands	340.774.5666
Utah	801.538.9600
Vermont	802.828.3171
Virginia	804 .786.2071 804.786.2042 or cybercrime@oag.state.va.us
Washington	360.753.6200 or 206.464.6684
West Virginia	304.558.2021 or 304.558.8986
Wisconsin	608.266.1221
Wyoming	307.777.7841 or 307.777.7874

000001-000001