



December 5, 2008

Office of the Attorney General  
Attn: Jan Myer  
900 E. Main Street  
Richmond, VA 23219

By UPS Express

**Subject: Notification Related to Virginia Code § 18.2-186.6(B)**

To Whom It May Concern:

Best Buy wishes to notify the Attorney General of an incident that occurred the week of November 10, 2008. It does not appear that the computer system security of Best Buy or its service provider was breached before, during or after the incident, and it may be that the provisions of Virginia Code § 18.2-186.6(B) do not apply. In keeping with the spirit of that law, however, we felt it appropriate to issue a notification concerning the incident to the 3 persons affected.

Best Buy uses a service provider named TALX Corporation ("TALX") to manage our payroll, W2 and related services. These services by their nature require TALX to store the social security numbers and, in some cases, the bank deposit details of our employees. On Tuesday, November 19, 2008, TALX notified us that they believed that the account information of three of our employees— 1 current and 2 former—was accessed by unknown persons using the account credentials of the affected employees. The account information accessed consisted of name, pay history, social security number, and direct deposit bank account information. The incident was reported to federal law enforcement agencies. According to our employment records, one of the persons affected by the incident, [REDACTED] is a resident of the Commonwealth of Virginia.

Based on our investigation it does not appear that the security of either Best Buy or TALX computer systems was breached in any way. This suggests that the account credentials of the affected employees were obtained through some type of malware or virus present on a computer that was used by an affected employee to access the TALX site.

Since the time the incident occurred, Best Buy and TALX have taken the following actions:

- Informed federal law enforcement authorities.
- Conducted an investigation of the incident.
- Disabled access to the accounts of the affected employees by forcing the expiration of the compromised passwords.
- Augmented the existing password-based online access control mechanism with an additional identity authentication technology based on Experian's Authentication Services (for more information see [http://www.experian.com/products/authentication\\_services.html](http://www.experian.com/products/authentication_services.html)).
- Attempted, beginning November 21, 2008, to contact the affected employees by phone and alert them to the incident, its nature and potential effect, and the steps that can be taken to prevent or reduce the risk

of identity theft. This notification was undertaken as soon as reasonably possible after we learned that it would not interfere with the investigative activities of federal law enforcement authorities.

- Sent on November 25, 2008, by UPS Next Day Air, a written notice of the incident to each of the affected employees, including Jimmy Hart. The notice sent to Jimmy Hart is enclosed with this letter for your convenience.

If you have questions concerning any matter contained in this letter, please consider me at your disposal.

Sincerely,

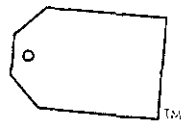
A handwritten signature in black ink, appearing to read 'Brad Bolin', with a long horizontal flourish extending to the right.

Brad Bolin  
Global Information Policy Counsel  
Best Buy Legal

(612) 291-6577 desk  
(952) 430-4916 fax

[brad.bolin@bestbuy.com](mailto:brad.bolin@bestbuy.com)

BTB/no  
Enclosure



**BEST BUY™**

November 25, 2008

[REDACTED]

Dear [REDACTED]:

Best Buy takes the security and privacy of your personal information extremely seriously. For this reason, we wish to notify you of an incident recently reported to us by one of our service providers. This letter is a follow-up to a phone call you should have received from our Employee Relations team.

Best Buy uses a service provider named TALX to manage our ePayroll, W2 and related services. On Tuesday, November 19, TALX informed us that they believe your account information was accessed by unknown persons using your username and password information. The account information accessed consisted of your name, pay history, social security number, and direct deposit bank account information.

The incident occurred the week of November 10. We notified affected individuals as soon as reasonably possible when it was clear that such notification would not impede ongoing law enforcement investigations.

Based on our investigation, it does not appear that the security of either Best Buy or TALX computer systems was breached in any way. This suggests that your user credentials were gotten through some type of malware or virus present on a computer that you used to access the TALX site. (NOTE: Accessing the TALX site from a Best Buy owned and issued computer system—such as a work laptop— would NOT have placed your username or password at risk, since these systems have continuously updated protective measures built into them.)

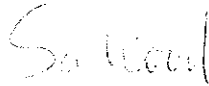
It appears your direct deposit bank account information was modified, presumably to redirect your pay to a different account. Best Buy recommends you immediately follow the list of steps below.

- Contact LifeLock, or other credit monitoring service of your choice, and enroll for their services. This service will provide you with a copy of your credit report in addition to placing fraud alerts on your file at all three major credit bureaus. The fraud alert signals creditors to take additional steps to verify your identity prior to granting credit in your name. This service can make it more difficult for someone to get credit in your name, though it may also delay your ability to obtain credit while the agency verifies your identity. Best Buy will reimburse the cost for up to 2 years of credit monitoring services.
- Contact your bank to close the account used for your direct deposit to ensure future fraud does not occur. Best Buy will reimburse the cost to open a new banking account and additional fees you may have as part of this process.
- To ensure your personal computer is free of the malware that may have caused this issue, you should have an anti-virus program implemented and running, make sure the anti-virus/spyware definitions are current and run a full scan. If you need help with these activities, we recommend you bring your personal computer into Geek Squad or another technical assistance company.
- For additional information on how to further protect yourself against identity theft, visit the website of the U.S. Federal Trade Commission at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft) or reach the FTC at 1-877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580.

If you have any questions or concerns as you take action to protect your identity, please contact Mindy Kirschman at 612-291-5644.

Again, we deeply regret any inconvenience or concern this incident may cause you.

Sincerely,



Sara Wood  
Director of Enterprise Privacy  
Best Buy

**UPS CampusShip: View/Print Label**

1. **Print the label(s):** Select the Print button on the print dialog box that appears. Note: If your browser does not support this function select Print from the File menu to print the label.
2. **Fold the printed label at the dotted line.** Place the label in a UPS Shipping Pouch. If you do not have a pouch, affix the folded label using clear plastic shipping tape over the entire label.

**3. GETTING YOUR SHIPMENT TO UPS**



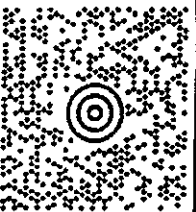
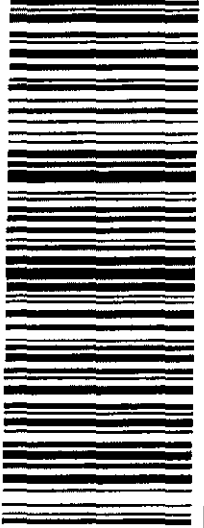

**Customers without a Daily Pickup**

- o Schedule a same day or future day Pickup to have a UPS driver pickup all your CampusShip packages.
- o Hand the package to any UPS driver in your area.
- o Take your package to any location of The UPS Store®, UPS Drop Box, UPS Customer Center, UPS Alliances (Office Depot® or Staples®) or Authorized Shipping Outlet near you. Items sent via UPS Return Services<sup>SM</sup> (including via Ground) are accepted at Drop Boxes.
- o To find the location nearest you, please visit the Resources area of CampusShip and select UPS Locations.

**Customers with a Daily Pickup**

- o Your driver will pickup your shipment(s) as usual.

FOLD HERE

<p>BETH ROBINSON 6122917411 BEST BUY CORPORATE HEADQUARTER 7601 PEGH AVENUE SOUTH RICHFIELD MN 55423</p> <p><b>SHIP TO:</b></p>  <p><b>RICHMOND VA 23234-2019</b></p> <p>LTR</p> <p>1 OF 1</p>	<p><b>VA 232 9-20</b></p>  	<p><b>UPS NEXT DAY AIR</b></p> <p><b>1</b></p> <p>TRACKING #: 1Z V9Y 228 01 9321 0537</p>		<p>BILLING: P/P</p> <p>Billing Info (Cost Center/GL number): 105 900010 980120</p> <p>CS 10-6-07. **000000 84-CA 10/2008</p>  <p>TM</p>
---	---	---	--	--