



American Postal Workers Union, AFL-CIO

1300 L Street, NW, Washington, DC 20005

Initiate National Dispute

Greg Bell, Director
Industrial Relations
1300 L Street, NW
Washington, DC 20005
(202) 842-4273 (Office)
(202) 371-0992 (Fax)

VIA FACSIMILE AND FIRST CLASS MAIL

March 3, 2008

Mr. Doug Tulino
Vice President, Labor Relations
U.S. Postal Service, Room 9014
475 L'Enfant Plaza
Washington, D.C. 20260

National Executive Board

William Burrus
President

Cliff "C. J." Guffey
Executive Vice President

Terry Stapleton
Secretary-Treasurer

Greg Bell
Industrial Relations Director

James "Jim" McCarthy
Director, Clerk Division

Steven G. "Steve" Raymer
Director, Maintenance Division

Robert C. "Bob" Pritchard
Director, MVS Division

Sharyn M. Stone
Central Region Coordinator

Mike Gallagher
Eastern Region Coordinator

Elizabeth "Liz" Powell
Northeast Region Coordinator

William "Bill" Sullivan
Southern Region Coordinator

Omar M. Gonzalez
Western Region Coordinator

Re: APWU No. HQTG20087, Postal Service Security Breaches of
Sensitive Data of Employees Related to Missing/Stolen Laptops

Dear Mr. Tulino:

In accordance with the provisions of Article 15, Section 2 and 4, of the Collective Bargaining Agreement, the American Postal Workers Union is initiating a Step 4 dispute concerning the Postal Service's data security breaches involving missing or stolen laptops (portable computing equipment) containing personal and confidential sensitive information of APWU bargaining unit employees, and related policies.

The issues and facts involved in this dispute are as follows:

By letter dated Dec. 1, 2006, the APWU was notified that the Postal Service was "developing a policy on data breach notification which will establish guidelines for evaluating incidents and determining appropriate response ... where it has been determined that the loss or compromise of sensitive personal data has occurred."

Since that date, the Postal Service has notified the APWU of at least thirteen (13) separate incidents of missing or stolen postal laptop computers that contained sensitive personal data of APWU bargaining unit employees, including (but not limited to) such items as name, home address, social security number, birth date, emergency contact information, and information concerning

EEO, Human Resources, Payroll, OWCP, FMLA, travel, and other personnel-related activities.

During this same time period, the APWU and the Postal Service have met repeatedly to exchange views regarding these incidents. The Union has repeatedly voiced our concerns regarding the apparent lack of security measures in place that can identify individuals who have access to and who store sensitive/confidential information on their laptops, and who are permitted to take this information, along with their laptops, off postal premises. Further, the Postal Service has been unable in any of the above cases, to identify the person or persons who authorized such individuals to store sensitive/confidential information on their laptops and take this information, along with their laptops, off postal premises, consistent with postal regulations found in the Handbook AS-805, *Information Security*.

It is the Union's position that the Postal Service has failed to take the necessary corrective action that would eliminate the danger related to these types of data security breaches by ensuring that no sensitive and private information is stored on laptops or other portable computing devices or removable media, especially social security numbers. The union has repeatedly expressed our skepticism of the business need, if any, for storing sensitive personal information, such as social security numbers, EID numbers, date of birth, home mailing addresses, etc. on portable and/or removable media, including laptop computers.

Furthermore, it is the Union's position that the Postal Service has taken entirely too long to notify employees when their personal information has been lost. The Union has raised our concerns on numerous occasions regarding the delays of anywhere from six to 12 weeks in notifying employees that their social security number may have been compromised. The U.S. Federal Trade Commission provides advice to businesses and individuals on preventing and dealing with identity theft that stresses the importance of taking steps promptly to guard against identity theft when there is reason to believe that sensitive information has been compromised. The Postal Service's delays in notifying employees that their personal information may have been compromised are unreasonable, and increases the risk of identity theft by delaying employees' ability to take preventive action.

In addition, the Union has repeatedly inquired what plans, if any, the Postal Service has to assist and/or compensate employees who become victims of identity theft as a result of a compromised Postal Service information resource. The Union believes that the Postal Service has an obligation as a responsible employer to provide identity theft insurance to employees whose personal information may have been compromised. The Union has provided the Postal Service with numerous examples of other responsible employers who provide Identity Theft Insurance for their employees in similar situations. The Postal Service's has been non-responsive to our numerous requests that impacted employees be provided identity theft insurance.

To date, nothing that has been said, nor information provided, dissuades the APWU from our belief that there is no business justification for storing employee social security numbers,

home addresses, dates of birth, and other sensitive data, on laptops and other portable computing devices, or for permitting such information to be taken off Postal Service premises.

It is the APWU position that the best business practice to ensure that there are no further breaches of security of this nature is for the Postal Service to discontinue the practice of storing sensitive data on portable computing equipment and permitting sensitive information to be taken off Postal Service premises.

Furthermore, it is the APWU position that impacted employees, i.e. employees whose personal sensitive information has been compromised as a result of the Employer's Security Data Breaches, should be provided by the Postal Service with identity theft insurance as soon as possible after their identity is determined.

Article 15 of the collective bargaining agreement provides that within thirty (30) days after the initiation of a dispute the parties shall meet in an effort to define the precise issues involved, develop all necessary facts, and reach agreement. It is requested that you or your designee contact my office at 202-842-4273 to discuss this dispute at a mutually agreed upon date and time.

Sincerely,


Greg Bell, Director
Industrial Relations

APWU #: HQTG20087

Dispute Date: 03/03/08

Case Officer: Greg Bell

Contract Article(s): 5; 19; AS-805

cc: Resident Officers

File

GB/BW