

American Postal Workers Union, AFL-CIO

1300 L Street, NW, Washington, DC 20005

Appeal to Arbitration, National Dispute

Greg Bell, Director
Industrial Relations
1300 L Street, NW
Washington, DC 20005
202-842-4273 (Office)
202-331-0992 (Fax)

September 12, 2008

VIA FACSIMILE AND FIRST CLASS MAIL

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

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

Re: USPS Dispute No. Q06C4QC08131428, APWU No. HQTG20087,
Postal Service Security Breaches of Sensitive Data of Employees
Related to Missing/Stolen Laptops

Dear Mr. Tulino:

Please be advised that pursuant to Article 15, Sections 2 and 4, of the Collective Bargaining Agreement, the APWU is appealing the above referenced dispute to arbitration.

Sincerely,

Greg Bell
Greg Bell, Director
Industrial Relations

USPS #: Q06C4QC08131428
APWU #: HQTG20087

Case Officer: Greg Bell
Step 4 Appeal Date: 3/3/2008
Contract Article(s): 5, Unilateral Action; 19,
Handbook or Manual Provisions; AS-805,
Information and Data Security;

cc: Resident Officers
Industrial Relations

File

GB/LB



American Postal Workers Union, AFL-CIO

1300 L Street, NW, Washington, DC 20005

Article 15 - 15 Day Statement of Issues and Facts

Sept. 12, 2008

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

Mr. Clifton Wilcox
Labor Relations Specialist
U.S. Postal Service
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: USPS No. Q06C4QC08131428, APWU No. HQTG20087,
Postal Service Security Breaches of Sensitive Data of Employees
Related to Missing/Stolen Laptops

Dear Mr. Wilcox:

On June 27, 2008, we met to discuss the above-referenced dispute at Step 4 of the grievance procedure. The parties mutually agreed to submit their written statements no later than Sept. 12, 2008. The following represents the APWU's understanding of the issues to be decided and the facts giving rise to the interpretive dispute.

This dispute concerns the Postal Service's security breaches of personal and confidential (sensitive) information of bargaining unit employees resulting from missing and/or stolen laptops. It is the APWU's position that, as an employer, the Postal Service has an obligation to safeguard such sensitive information. When it fails to do so, affected employees' rights under the Privacy Act and applicable postal regulation are violated. It is also the APWU's position that, as a remedy, the "best business practice" should be applied and that identity theft insurance be provided to impacted employees as soon as possible after it is determined that their sensitive personally identifiable information may have been compromised.

To date, nothing has been provided by the Postal Service to dissuade the APWU 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. Moreover, the “best business practice” to ensure that there is no further breach of security of this nature is to discontinue the practice of storing sensitive data on portable computing equipment and permitting sensitive information to be taken off Postal Service premises.

In regard to our inquiry concerning 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 Postal Service simply takes the position that: *“To date, no reports of Identity Theft related to lost or stolen equipment or otherwise have been reported. If a case of Identity Theft related to a reported incident does occur, the Postal Service will determine what steps are appropriate.”*

Naturally, the APWU is pleased that, to date, there are no reports of identity theft related to a lost or stolen Postal Service information resource, but the purpose of Identity Theft Insurance is to have it in the event identity theft related to a reported incident does occur. The Postal Service has refused the Union’s request to provide Identity Theft Insurance to impacted employees as soon as possible after it is determined that an employee’s sensitive personally identifiable information may have been compromised.

Background

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 seventeen (17) separate incidents of missing or stolen Postal Service 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*. They have repeatedly claimed that the AS-

805's requirement for written acknowledgment and acceptance of the risks associated with each sensitive, critical or business controlled information resource, as described in the AS-805's Information Resource Risk Management policy, is inapplicable to the uses associated with these incidents, without any explanation of why it is not applicable.

In addition, in each of the above cases, the Postal Service has failed to identify the "business need" that allegedly necessitated the storage of sensitive employee data on a portable computing device. The Postal Service has limited their justification of this practice to a general statement concerning "considerations which include the business-controlled criticality of many information resources essential for uninterrupted Postal Service operations, and/or the protection of the health and safety of all personnel...." They have consistently failed to demonstrate or even attempt to explain the need for storing sensitive information on portable computing devices in any specific case.

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, particularly in light of the clear policy statement of the Postmaster General in a letter to all employees dated July 12, 2006 on the subject of "Securing Sensitive Business and Personal Information."

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.

The remedy requested by the union includes, but is not limited to the following: that the Postal Service immediately cease and desist from storing sensitive employee data, especially social security numbers, on portable computing devices or other portable media, and that impacted employees be provided with the strongest possible identity theft protection including, but not limited to, identity theft insurance and/or other identity theft

Re: Q06C4QC08131428
September 12, 2008
Page 4

protection services, as soon as possible after it is determined that their sensitive personally identifiable information may have been compromised.

Sincerely,


Greg Bell, Director
Industrial Relations

APWU #: HQTG20087
USPS #: Q06C4QC08131428

Dispute Date: 3/3/2008
Contract Articles: 5, Unilateral Action; 19,
Handbook or Manual Provisions; AS-805,
Information and Data Security;

cc: Industrial Relations

GB/LB



September 12, 2008

Mr. Greg Bell
Director, Industrial Relations Division
American Postal Workers
Union, AFL-CIO
1300 L Street, NW
Washington, DC 20005-4128

RE: Q06C-4Q-C 08131428
Washington, DC 20260

Dear Greg:

On July 7, we met to discuss the above-captioned dispute which is pending at the fourth step of our grievance/arbitration procedures. Since the parties have been unable to resolve this pending dispute, in accordance with Article 15.2.Step 4, this constitutes the Postal Service's understanding of the issues involved and the facts giving rise to the interpretive dispute.

Interpretive Issue Presented

Whether allowing laptop computers that potentially contain personal, confidential, and/or sensitive information of APWU employees off postal premises violates postal regulations.

Background

By letter dated December 1, 2006, the Postal Service notified the APWU that it was developing a policy on documenting information security requirements for portable media devices that leave postal premises and the data it contains. Since that date, the Postal Service notified the APWU of at least thirteen (13) separate incidents where portable media devices off postal premises were missing or stolen and potentially contained APWU employee data. On September 5, 2007, the Postal Service implemented PS Form 1357-D, *Data Accountability*. The PS Form 1357-D formally documented management authorization for access to Postal Service laptops or other portable media devices. The form documents individual responsibility for the security of the computing equipment and the data that it contains, and is used to authorize Postal Service computing equipment off premises. The PS Form 1357-D reiterates that employees are aware of their responsibility for securing sensitive data and the need to immediately report any missing equipment to the proper authorities.

APWU Position

The APWU alleges that the Postal Service has violated security policies when allowing portable media devices to be taken off Postal Service premises that potentially contain APWU bargaining unit employees' personal or sensitive information.

In sum, it is APWU's position that the Postal Service has failed to take the necessary corrective action that would eliminate the danger related to missing or stolen portable media devices by authorizing these computer devices that potentially contain APWU bargaining unit employees' personal or sensitive information off postal premises. Additionally, the Union alleges that the Postal Service takes too long to notify employees and the Union when portable media devices that are off Postal Service premises are missing or stolen. As a remedy, the APWU believes that the Postal Service has an obligation to provide identity theft insurance to employees whose personal information may have been compromised.

USPS Position

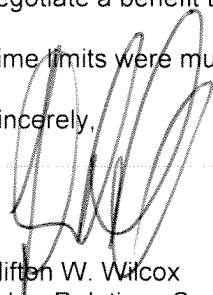
The Postal Service's position is that the privacy and security of data, on or off postal premises, is of the utmost importance. When portable media devices leave postal premises the information contained in the device is secure through the security protections installed on devices. Additionally, it is the Postal Services position that information stored on these portable devices are encrypted and would make it difficult for unauthorized individuals to access the information on these devices without the proper authorization. When incidents occur that involve portable devices, on or off postal premises, the affected employees were individually advised of the incidents and provided information resources regarding precautionary protective measures against identity theft.

Since September 5, 2007, the Postal Service has used the PS Form 1357-D, as a method to formally document security requirements for portable media devices that leave postal premises and the data it contains. Additionally, the Postal Service continues to use encryption technology that uses a unique identification and password for further protection. When incidents occur, on or off postal premises, the Postal Service investigates each incident to determine the extent, if at all; that personal information was contained in the missing or stolen portable media device. Once the investigation has determined personal information was contained on the missing portable media device, the employee and the Union representing the employee would be notified in writing.

As a remedy, the APWU insists that the Postal Service assist and/or compensate employees who become victims of identity theft by providing identity theft insurance to employees whose personal information may have been compromised from portable media devices taken off postal premises. It is the Postal Service's position that identity theft exists in various forms. Identity theft could exist as a result of an APWU employee being careless or reckless with his or her own personal information through a lost wallet, purse, or personal information exchanged over the Internet. To date, the APWU has not shown where a nexus exists between lost or stolen portable media devices taken off postal premises and the theft of identity of APWU employees. Therefore, the Postal Service has determined that identity theft insurance is not warranted. Additionally, it is the Postal Service's position that identity theft insurance is a benefit that should be negotiated, bargained for, between the parties. Therefore, the APWU is attempting inappropriately to negotiate a benefit through the grievance/arbitration process.

Time limits were mutually extended for the exchange of 15-day letters.

Sincerely,



Clifton W. Wilcox
Labor Relations Specialist
Contract Administration (APWU)