IN THE MATTER OF THE ARBITRATION BETWEEN

GRIEVANCE NO.: 34-11-100625-0127-01-09

The Ohio Civil Service Employees

Association, AFSCME Local 11

#1079

GRIEVANT: Kimm Gorman

AND

Ohio Bureau of Workers Compensation

OPINION AND AWARD
ARBITRATOR: Meeta Bass Lyons

AWARD DATE: April 21, 2011

APPEARANCES FOR THE PARTIES

MANAGEMENT:

Bradley A. Nielsen, Labor Relations Officer, First Chair

Aimee Szczerbacki , Office of Collective Bargaining, Second Chair

UNION: Jennie Lewis, Ohio Civil Services Employees Association, AFSCME Local 11, First Chair

Michael Gee, Ohio Civil Service Employees Association, Second Chair

Grievant, Kimm Gorman

PROCEDURAL HISTORY

The Ohio Bureau of Workers Compensation is hereinafter referred to as "Employer" or "BWC". The Ohio Civil Service Employees Association, AFSCME, Local 11 is hereinafter referred to as "Union". Kimm Gorman is the Grievant.

Grievance No. 34-11-100625-0127-01-09 was submitted by the Union to Employer in writing on June 25, 2010 pursuant to Article 24 of the parties' collective bargaining agreement. Following unsuccessful attempts at resolving the grievance it was referred to arbitration in accordance with Article 25, Section 25.03 of the 2009-2012 Collective Bargaining Agreement.

Pursuant to the collective bargaining agreement between the Union and Employer, the parties have designated this Arbitrator to hear and decide certain disputes arising between them. The parties presented and argued their positions on February 7, 2011 in Columbus, Ohio. During the course of the hearing, both parties were afforded full opportunity for the presentation of evidence, examination and cross-examination of witnesses, and oral argument. Witnesses were sequestered during the hearing. Parties agreed to submit written closings on or before March 21, 2011.

The parties stipulated that the grievance and arbitration were properly before the Arbitrator. The parties did stipulate to the issue as follows: Did the Ohio Bureau of Workers' Compensation possess just cause to remove BWC Fraud Investigator Kimm Gorman from employment? If not, what shall the remedy be?

PERTINENT PROVISIONS OF THE 2009-2012 AGREEMENT

ARTICLE 24
24.01 - Standard
Disciplinary action shall not be imposed upon an employee except for just cause. The Employer has the burden of proof to establish just cause for any disciplinary action. In cases involving termination, if the arbitrator finds that there has been an abuse of a patient or another in the care or custody of the State of Ohio, the arbitrator does not have authority to modify the termination of an employee committing such abuse. Abuse cases which are processed through the Arbitration step of Article 25 shall be heard by an arbitrator selected from the separate panel of abuse case arbitrators established pursuant to Section 25.04. Employees of the Lottery Commission shall be governed by ORC Section 3770.02(1).

24.02 - Progressive Discipline

The Employer will follow the principles of progressive discipline. Disciplinary action shall be commensurate with the offense. Disciplinary action shall include:
a. One (1) or more oral reprimand(s) (with appropriate notation in employee's file);
b. One (1) or more written reprimand(s);
c. One (1) or more working suspension(s). A minor working suspension is a one (1) day suspension, a medium working suspension is a two (2) to four (4) day suspension, and a major working suspension is a five (5) day suspension. No working suspension greater than five (5) days shall be issued by the Employer.
If a working suspension is grieved, and the grievance is denied or partially granted and all appeals are exhausted, whatever portion of the working suspension is upheld will be converted to a fine. The employee may choose a reduction in leave balances in lieu of a fine levied against him/her.
d. One (1) or more day(s) suspension(s). A minor suspension is a one (1) day suspension, a medium suspension is a two (2) to four (4) day suspension, and a major suspension is a five (5) day suspension. No suspension greater than five (5) days shall be issued by the Employer;
e. Termination.
Disciplinary action shall be initiated as soon as reasonably possible, recognizing that time is of the essence, consistent with the requirements of the other provisions of this Article. An arbitrator deciding a discipline grievance must consider the timeliness of the Employer's decision to begin the disciplinary process.
The deduction of fines from an employee's wages shall not require the employee's authorization for withholding of fines.
If a bargaining unit employee receives discipline which includes lost wages, the Employer may offer the following forms of corrective action:
1. Actually having the employee serve the designated number of days suspended without pay;

2. Having the employee deplete his/her accrued personal leave, vacation, or compensatory leave banks of hours, or a combination of any of these banks under such terms as may be mutually agreed to between the Employer, employee, and the Union.

BACKGROUND

Set forth in this background is a summary of undisputed facts and evidence regarding disputed facts sufficient to understand the parties' positions. Other facts and evidence may be noted in the discussion below to the extent knowledge of either is necessary to understand the Arbitrator's decision.

Grievant commenced employment with the State of Ohio at the Ohio Bureau of Workers' Compensation (BWC) on November 23, 1998. At the time of her removal, Grievant was a fraud investigator for Special Investigations Department (SID) assigned to the Automated Detection and Intelligence (AD&I) team. SID is designated as the Ohio criminal justice agency that is responsible for the pursuit of claims fraud, medical provider fraud and premium fraud. As a fraud investigator, Grievant was responsible for working on detection projects and out of state wage requests, providing support to field investigators by completing data runs, conducting queries in law enforcement databases such as Accurint, LEADS (Law Enforcement Data System) and creating provider databases and analyzing data. SID cases that establish fraud are forwarded for prosecution, and there is likelihood that the investigator is called as a witness.

Accurint is software that is specifically designed for state and federal law enforcement entities. The contract between BWC and Accurint, "Limits Accurint services to the performances of, or in the furtherance of law enforcement activities, including without limitation, criminal investigations, witness location, and other purposes reasonably related to provision of law enforcement by the Agency." The software provides background information

of an individual including but not limited to convictions, former employers, social security numbers, driver's license information, addresses, vehicle information, and so forth. BWC runs an Accurint search on prospective employees working in the unclassified service as part of the background check performed prior to offering employment.

In addition to the background check completed through the Accurint system, SID runs a credit report and score of the prospective applicant. This information is stored in the employee's background check folder. AD&I Team maintains databases and queries the claim information on former BWC employees. Former BWC employee names, social security numbers and other confidential information are maintained by the BWC in these files. Grievant had the ability to access all of said information as a fraud investigator.

Grievant filed a hostile work environment complaint with the BWC Human Resources Office on May 12, 2010. The complaint arises from a belief held by Grievant that Employer failed to properly handle an on-going incident between Grievant and another female coworker involving an exchange of emails, facial expressions between the two, conversation between others within earshot of Grievant, loud statements and comments with a racial overtone. The complaint was subsequently referred to SID Threat Assessment Coordinator Reitz for investigation. The investigator found no merit to the allegations of workplace violence or hostile work environment by Gorman, and recommended that the case be closed. The investigator recommended that issues be addressed by supervisors at the time they are made.

The work activity of Grievant was placed under surveillance. On May 25, 2010, Grievant accessed and viewed the confidential information of Investigator Reitz, information contained in a SID background check folder. On May 25, 2010, Grievant viewed a file containing the confidential

information of former BWC employees. There was no business related purpose for viewing the confidential information of Investigator Reitz. Grievant stated that she accidentally entered into the personal folder and files of Investigator Reitz. Grievant is not responsible for background checks for AD&I.

Employer placed Grievant on paid administrative leave on June 1, 2010. Employer removed Grievant from employment on June 18, 2010. Grievant was removed on June 18, 2010 for violations of the BWC Disciplinary Policies to wit, insubordination, failure to follow a written policy of the employer & dishonesty, intentionally making false or untrue statements regarding work related matters to management, fellow employees or the public, and intentional misuse, destruction, defacing of state property, public property or property of another for example LEADS. Grievant did not possess any active discipline at the time of her removal.

The Union filed its grievance on June 25, 2010 alleging a violation of Article 24 and 2 of the Collective Bargaining. The grievance was not resolved within the procedure established by the collective bargaining agreement, and was properly advanced to arbitration.

POSITION OF EMPLOYER

Employer contends that the Grievant violated BWC Memo 4.35 –BWC Computer Security Acceptable Use Policy. Grievant utilized her BWC assigned computer to access confidential files containing the personal/confidential/sensitive information of Investigator Reitz and former BWC employees without a business related purpose. A BWC employee must avoid not only the impropriety, but the appearance of impropriety. By accessing the personal/sensitive/confidential information of current and former BWC employees without a business related purpose, Grievant violated the BWC Code of Ethics Memo 1.01. There is just cause to discipline.

Employer contends that by accessing the confidential/personal/sensitive information of investigator and former BWC employees without a business related purpose, the Grievant intentionally misused the Accurint software. By misusing the Accurint information, Grievant exposed the BWC to a potential breach of contract and jeopardized the BWC's continued ability to utilize the software.

Employer contends Grievant was dishonest in her investigatory interview on June 11, 2010. Prior to commencing the investigatory interview, Employer provided Grievant with a direct order to answer all questions honestly and accurately. When specifically asked if Grievant accessed the background check folder and the investigator 's background check folder, the Grievant responded that she accidentally clicked on the folders and that as soon as she realized what she did, she left the folders. These were untruthful responses to both questions. Her actions were intentional as evident through the methodical viewing of every file contained in the background check

folder. Because of its status as law enforcement Agency, Employer terminates the employment of any employee guilty of dishonesty.

Employer requests that Grievance No. #34-11-100625-0127-01-09 be denied.

POSITION OF UNION

Union contends that Employer failed to establish that Grievant was dishonest in her investigatory interview. Grievant in her position as a fraud investigator had access to employees' folders, and said access was essential to her work as a fraud investigator. Grievant never denied entering the personal folder of the investigator. Grievant explained that she was "clicking really fast." When Grievant realized where she was in the system, she left the area. The responses of Grievant do not rise to the level of dishonesty.

Union contends that Grievant had over twelve years of state service with no active disciplines at the time of termination. Her performance evaluation just prior to the alleged incident was satisfactory. Her removal is excessive when she accidentally accessed the information. The discipline was not progressive.

Union contends that the discipline imposed by Employer was excessive. Grievant never printed, faxed, emailed, copied, scanned or memorialized any information which he had seen in an employees' file. The mere fact Grievant accidentally accessed an employee's file does not warrant termination when there was no evidence of dissemination of the information.

Union requests that Grievance No. #34-11-100625-0127-01-09 be sustained, and Grievant returned to her position and warded back pay, reimbursed any medical or hospital expenses incurred during the period

from the date of the removal to the date of reinstatement. Restore her seniority, leave balances that Grievant had at the time of the removal and those she would accrued since her removal, made whole and awarded any other remedies deemed appropriate.

DECISION

Article 24.01 of the 2009-2012- Collective Bargaining Agreement provides in pertinent part that "Disciplinary action shall not be imposed upon an employee except for just cause. The Employer has the burden of proof to establish just cause for any disciplinary action." The just cause standard of review requires consideration of whether an accused employee did in fact violate or disobey a rule or order of management. If a violation is proven, other considerations relate to fairness and whether the severity of disciplinary action is reasonably related to the seriousness of the proven offense and the employee's prior record.

Grievant is charged with a violation of BWC Disciplinary Policy Insubordination: Failure to follow a written policy of the Employer. The policies at issue are the BWC Computer Security Acceptable Use Policy, Memo 4.35, and Memo 1.01. The overview of the policy in Memo 4.35 states that "Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operations systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of BWC. These systems are to be used for business purposes in serving the interests of the company and our customers in the course of normal operations." Specifically, Section 4.3(7) Unacceptable Use, System and Network Activities states that effecting security breaches or disruptions of network communications are prohibited. Security breach is defined as accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly

authorized to access, unless these duties were within the scope of regular duties. The BWC last provided an update to the Grievant on Memo 4.35 in December 2007, and the Grievant acknowledged receipt.

Memo 1.01 is a recitation of Chapter 4123.15 Ethics Rules, and establishes the code of ethics for BWC. An employee who violates any provisions in the code of ethics is subject to discipline. Section 4123-15-03 (B) (j) states that an employee is prohibited from the use or disclosure of confidential information protected by law, unless appropriately authorized. Section 4123-15-03 (H) states that the confidentiality of all information which comes into possession of BWC shall be respected. Grievant acknowledged receipt of Memo 1.01 on February 20, 2008.

On May 10, 2010, Grievant by signature acknowledged that she had read and understood the department's confidentiality statement which states "it is the policy of the BWC Special Investigations Department (SID) to maintain the confidentiality of information, ensuring no information is released or revealed to any person not privileged to that information."

Additionally, when Grievant clicks to enter the website link to access the Accurint search database, the link is clearly identified for law enforcement purposes only. The website Page was replicated at Tab Thirteen of the binder. One screen is entitled *Permitted Use Certification*, and the subheading states, "This service may contain information governed by the Gramm-Leach–Biley Act (GLBA). In accordance with the GLBA, please select the purpose for which you intend to utilize this information. The purposes you select govern this entire session. If the purpose for which you are conducting searches changes, you will need to exit the system, re log-in, and select another purpose." The footnote further states: "You hereby agree to use these services in accordance with applicable law including the permissible use selection and agree that failure to do so will be a breach of your agreement for this service. Laws applicable to use of this product

include the Drivers' Privacy Protection Act and related state laws (DPPA) and the Graham –Leach-Biley Act (GLBA). The data regulated by the DPPA and the GLBA may be used only for the permissible uses that you select below. By selecting a permissible use, you are certifying that the date returned to you will be used for that purpose. The date provided to you by use of this product may not be used as a factor in establishing a consumer's eligibility for credit, insurance, employment or other identified under the Fair Credit Reporting Act (FCRA)." Similar language is found at Driver's Privacy Protection Act of 1994 (DPPA). It is not disputed that the Grievant is responsible for running/obtaining Accurint reports for field staff, thus she views the law enforcement purpose notice every time she logs in to run a report.

Grievant had ample notice of the confidentiality rules. There was no dispute that the rules was reasonable and serves a legitimate business interest of Employer.

Grievant testified that she accidentally accessed the personal folder of Investigator Reitz assigned to her hostile environment complaint. When she realized where she was, she backed out of the folder. Management disputes that her access into the personal folder of the investigator was an accident, and maintains that her actions were deliberate. Management introduced evidence of her computer screen shots captured by BWC Cyber Crimes Unit. The computer surveillance shows the folder and files accessed by Grievant, the number of clicks to enter said files, and the scroll down of several pages of a sixteen page document viewed by Grievant.

Grievant made the following statements during her investigatory interview:

Question 12. You have not conducted background checks for ADI, correct?

Response. Correct.

Question 13. Who is responsible for running the background checks for ADI?

Response: I have no idea.

Question 14. Have you completed any background checks for ADI?

Response: No, ADI, no.

Question 15. Would you have any reason to review any of the background checks in this file?

Response: No.

The explanation of Grievant that she was clicking very fast, and when she saw where she was, she backed out, as an accidental access into said personal folder and files, lacks credibility. Grievant had no business-related purpose to access the personal record of Investigator Reitz.

Additionally, Grievant had accessed a query of former BWC employees which was not a current project of Grievant. Grievant explained that she had been working on a drug project that she had submitted to her supervisor back in April of 2009 after reading a newspaper article regarding deaths involving overdose of prescription drug use. Grievant returned from disability leave the latter part of April of 2010. On May 25th Grievant noticed that her coworker was having a meeting on matters related to Grievant's drug project, and Grievant was not asked to attend. Grievant then searched her computer for her project, and found her project in the fraud ADT folder. There was insufficient evidence to find by clear and convincing evidence that there was no business-related purpose to the access of this information.

Grievant is charged with dishonesty, intentionally making false or untrue statements regarding work related matters to management, fellow employees or public. Management conducted an investigatory interview on June 1, 2010. The opening paragraph of the document states that "As in any investigation conducted by the Bureau, we expect our employees to answer

honestly and fully. Because of the serious nature of investigatory interviews, we must issue a direct order to answer these questions fully and accurately." Further Grievant signed that statement therein which states that "I, Kimm Gorman, acknowledge that I have been advised of the disciplinary nature of this meeting and that I have been given a direct order to answer the questions honestly and accurately. I understand that I could be subject to further discipline if I fail to comply with that direct order."

The screen shots of her computer surveillance establish that she intentionally accessed the personal folder of Investigator Reitz. Consequently when asked: Have you accessed the file entitled Background Checks? Grievant's response "I think I accidentally clicked on it. When I realized what I was in I came out of it," is a false statement. And when asked: Did you access Art Reitz's background check folder? The last two statements of Grievant's response "I know when I was clicking really fast; I clicked on Art's, *when I realized where I was at. I came out,"* is also a false statement. Grievant may have been clicking fast, but she intentionally selected, accessed and viewed the confidential information of Investigator Reitz. By making these false statements to management, Grievant violated the rule.

Having determined that the violations occurred, the next question becomes whether or not the penalty imposed, removal, was reasonably related to the seriousness of the offense in consideration of the employment record of Grievant. The disciplinary options for a first offense for all the violations are determined based upon the severity of the incident. The policy allows for discharge if appropriate for even a single violation by an employee with no prior discipline.

Union argues that since the information was not misused or disclosed to anyone who did not have access, removal is excessive. The confidential information of the employees was not printed, faxed, scanned or copied. In

support of its position, the Union submits the opinion and award of *In Re The Franklin County(Ohio) Sheriff's Office and the Fraternal Order of Police Capital City Lodge No. 9*, 124LA 654 (November 29, 2007). The facts in this arbitration involved a police officer who accessed personal information on his girlfriend through LEADS, ran a LEADS check to support a bogus traffic stop, and ran a LEADS check on the alleged father of one of his girlfriend's children to determine if a warrant had been issued on him for nonsupport. Arbitrator Bell found that accessing LEADS on the occasions stated above did not constitute an "unlawful utilization of leads, for he did not use such information for the support of illegal activities nor did he disseminate the information so accessed. Arbitrator Bell found the actions constituted an abuse of computer resources *for which other deputies were given a one-day suspension.* (Emphasis Added) Arbitrator Bell did not make a determination of the remedy for the misuse of computer resources; past practices established that for him. In the instant grievance, Grievant is charged with the intentional misuse, destruction, defacing of state property, public property or property of another, when Grievant conducted her own in-house back ground check of the investigator for her own personal knowledge, Grievant misused his property.

Grievant is charged with dishonesty and insubordination. Employer has established by clear and convincing evidence, Grievant engaged in the conduct, which constitutes insubordination and dishonesty as defined in the policy. Grievant had notice of the policies. Employer determined in its grid that the penalty for this particular type of conduct, insubordination and dishonesty, would be determined based upon the severity of incident. In consideration of the nature of the offense, the quasi criminal nature of its operations, the duties related to the position, and the effect on outside contracts, the Employer determined that removal was the appropriate

remedy. In dishonesty cases, Employer has administered the discipline even-handedly. There is a reasonable relationship between Grievant's misconduct and the punishment imposed. Grievant was trusted to perform her duties and to respect the personal/sensitive/confidential information of BWC employees. Grievant accessed personal/sensitive/confidential information without any business related purpose. The Grievant was a twelve year employee with no active discipline. But, the seriousness of this offense, accessing personal/sensitive/confidential information for personal knowledge overshadows her work record and tenure.

In summary, the evidence persuades the Arbitrator that Grievant violated the following work rules: Insubordination (b) Failure to follow a written policy of the employer; Dishonesty (a)Intentionally making false or untrue statements regarding work-related matters to management, fellow employees or the public and (d) Intentional misuse, destruction, defacing of state property, public property or property of another employee (e.g., Law Enforcement Automated Data Systems (LEADS), as alleged in Employer's letter of June 18, 2010. And discharge was not so excessive a punishment as to be beyond the Employer's managerial prerogatives. The Arbitrator concludes discharge of the Grievant was for just cause. The Arbitrator must therefore deny Grievance no. 34-11-100625-0127-01-09.

AWARD

After a full review and consideration of all documents and arguments presented, as well as the testimony of witnesses, and the post hearing briefs of the parties, Grievance No. #34-11-100625-0127-01-09 is denied.

April 22, 2011

/s/Meeta Bass Lyons
Meeta Bass Lyons, Arbitrator
Steubenville, Ohio