

**BEFORE THE MERIT EMPLOYEE RELATIONS BOARD
OF THE STATE OF DELAWARE**

GRIEVANT,)	
)	
Employee/Grievant,)	
v.)	DOCKET No. 15-10-638
)	
DEPARTMENT OF HEALTH AND SOCIAL)	DECISION AND ORDER
SERVICES/DIVISION OF MANAGEMENT)	
SERVICES,)	<i>[Public – redacted]</i>
)	
Employer/Respondent.)	

After due notice of time and place, this matter came to a hearing before the Merit Employee Relations Board (the Board) at 9:00 a.m. on March 17, 2016 in the Farmington-Felton Conference Room, at the Delaware Department of Transportation, located at 800 S. Bay Road, Dover, DE 19901. The hearing was closed to the public, pursuant to 29 Del.C. §10004(b)(8).

BEFORE Martha K. Austin, Chair, Jacqueline Jenkins, Ed.D, Victoria Cairns, and Paul Houck, Members, a quorum of the Board under 29 *Del. C.* §5908(a).

APPEARANCES

Rae M. Mims
Deputy Attorney General
Legal Counsel to the Board

Deborah L. Murray-Sheppard
Board Administrator

Gerry Gray, Esq.
on behalf of the Grievant

Kevin R. Slattery
Deputy Attorney General
on behalf of the Department of
Health and Social Services

BRIEF SUMMARY OF THE EVIDENCE

The Department of Health and Social Services, Division of Management Services (“DMS”) offered and the Board admitted into evidence without objection 26 exhibits marked for identification as A-Z. An additional item was entered into the record on rebuttal which was marked as AA. DMS called two witnesses: Heather Morton (“Morton”), Controller II, DMS; and Harry Roberts (“Roberts”), Chief of Administration, DMS.

The employee/grievant (“Grievant”), offered and the Board admitted into evidence without objection 20 exhibits marked for identification as 1 - 20. The Grievant testified on her own behalf.

FINDINGS OF FACT

The Grievant worked as an accounting specialist in the payroll unit at DMS for seven years prior to being terminated from her employment on September 4, 2015. The primary responsibility of an accounting specialist includes entering timekeeping and payroll records for the Department’s employees in an accurate and timely manner into the Payroll/Human Resource Statewide Technology (PHRST)¹ system.

There were four employees who worked in the payroll accounting unit at the time of the incident, including the Grievant. For purposes of this decision, the other three employees are identified simply as MR, CK and AS, as there are other related grievances which are currently pending. CK held the position of Accountant, while the other employees held Accountant Specialist positions. It was established that CK, MR, and AS were friends, and the Grievant considered them a clique.

¹ PHRST, a statewide system, allows staff to enter, update, modify, delete, retrieve/inquire and report data in three areas: human resource, benefits and payroll by the data entry dates specified by the State of Delaware.

The State payroll system defaults at 75 hours per two week pay period (which ends on Saturday). Overtime worked must be authorized and is reported to the payroll office through the use of an “exceptions report”. The information on the exceptions report is manually entered into the PHRST system by an accounting specialist. When the information has been entered, the accounting specialist who enters the data, verifies it by writing a hash mark and her initials on the exception report. A second hash mark and set of initials is entered by the individual who is conducting the quality assurance review. The review occurs the same day or as soon as possible after the initial entry is keyed into the system (usually by not later than Wednesday afternoon). DMS normally finalizes its payroll and sends it over to be paid on the following Friday, approximately two days after the data has been entered.

PHRST will not allow Accountant Specialists to enter their own time. All Accountant Specialists receive training on PHRST and receive a unique identification and password to gain access to the system.

In June, 2015, an issue concerning payment for unauthorized overtime was brought to the attention of the DMS Controller (“Morton”) by the Grievant’s supervisor. Morton testified she received an email on June 18, 2015 from a Fiscal Administrative Officer who related that the Grievant had expressed concerns to him that the department’s overtime policy was not being enforced fairly in the payroll unit. The Grievant was upset that both she and MR had been denied authorization for overtime they had worked because they did not have the required back-up documentation to be paid overtime. The Grievant had entered MR’s payroll information (without payment for overtime) and it had been checked by another employee who was responsible for quality control. The Grievant was able to go into the PHRST system after the pay checks had been issued to view MR’s pay check, at which time she found that MR had been paid for the unauthorized overtime. The Grievant reported to the fiscal office that she believed

MR's payroll records had been changed after the Grievant had entered it and it had been checked by quality control.

During the initial investigation, Morton was able to confirm that MR had received unauthorized overtime, as alleged. DMS did not approve any overtime payment for MR on the exception report for that pay period. Pay check records, however, revealed (consistent with the Grievant's report) that MR had been paid for five hours of overtime at her straight time rate and 8.75 hours of overtime at time-and-a-half. The payout resulted in an additional \$293.63 in MR's pay check.

Morton was also able to determine that CK had received a large amount of overtime during the same pay period that was also not supported by an exception report. The exceptions report for CK included approval for 2.5 hours of overtime at her straight time rate and 1 hour of overtime at time-and-a-half times her straight time rate. She was paid, however, for 5 hours of straight overtime and 5.25 hours of overtime at time-and-a-half. In addition, she received 2.5 hours of straight overtime, 29.75 hours of overtime at time-and-a-half and 7.50 hours of holiday pay. This resulted in CK receiving an additional \$1100 in her pay check.

The records indicated the changes to the timekeeping records of both MR and CK were made by the Grievant after the quality control review had been completed. No modifications were listed in the documentation after the Grievant's entries.

Based on this information, Morton initiated a full investigation into the payroll records for all DMS employees in New Castle County, focusing on over time paid in FY 2014 and FY 2015. The investigation included review of exception reports, payroll/pay check reports and a PHRST audit trail. The investigation revealed similar types of transactions for the following pay periods: November 16, 2013; October 4, 2014; October 18, 2014; November 1, 2014; November 15, 2014; November 29, 2014; December 13, 2014; December 27, 2014; January 10,

2015; January 24, 2015; February 7, 2015; February 21, 2015; March 7, 2015; March 21, 2015; April 4, 2015; April 18, 2015; and May 2, 2015. In total, CK received \$13,077.62 in unauthorized overtime payments.

Overtime payments to CK and MR keyed in under the Grievant's user identification occurred for close to eight months. According to payroll records, the Grievant never received additional overtime payments nor did she receive any other financial gain that was revealed through the investigation.

The Grievant's identification along with a password of her own construction allowed her entry to PHRST. The system requires passwords be changed every 90 days and it only allows three attempts to use a password. According to Morton, the PHRST audit trail does not provide the option to identify at which computer information was entered using specific user identification.

The Grievant testified she began doing payroll on or around March 2012. The Grievant testified she never gave her password to anyone, never wrote down her password, she routinely changed it and she is aware of the policies and procedures for safeguarding her identification and password. The Grievant had a small office with a door like the other employees in her unit. Her desk faced the door and there was a chair next to the desk. She testified she locked her computer whenever she left her desk. DMS took photographs of the Grievant's desk which showed various post-it notes featuring what appeared to be passwords.

At the conclusion of the investigation, DMS management recommended the Grievant be terminated. The Grievant was advised on August 5, 2015, of the recommendation and of her right to a pre-termination hearing prior to a final decision in the letter. The pre-termination letter stated the investigation uncovered unauthorized transactions to CK and MR which violated the public trust and reflected unfavorably on the State. Specifically, DMS cited three violations

as the bases for the termination:

- 1) Violation of the State's Code of Conduct:
Each state employee, state officer and honorary state official shall endeavor to pursue a course of conduct which will not raise suspicion among the public that such employee, state officer, honorary state official is engaging in acts which are in violation of the public trust and which will not reflect unfavorably upon the State and its government.
29 Del. C. § 58806
- 2) Violation of DHSS Policy Memorandum #3, Appropriate Use of DHSS Information Technology:
It is expected that users will conduct State of Delaware business with integrity, respect and prudent judgement while upholding the state's commitment to the highest standard of conduct.
- 3) Violation of the Department of Technology and Information's ("DTI") Acceptable Use Policy:
All staff is personally responsible for information security...All staff has the following responsibility: Compliance with the State of Delaware Information Security Policies, procedures and standards established to maintain the confidentiality, integrity and availability of State information and data assets; protecting the secrecy of their password; and participating in annual information security awareness training.

In a letter dated September 4, 2015 the cabinet secretary informed the Grievant she agreed with the recommendation to terminate the Grievant's employment. The secretary noted no new or mitigating information was provided at the pre-termination meeting, and concluded that the Grievant either entered the payroll information for CK and MR, or (at the very least), recklessly allowed her user ID and password to be accessed and utilized in a fraud scheme involving her coworkers. This caused a breach of protocol that resulted in financial losses to the State.

CONCLUSIONS OF LAW

Merit Rule 12.1 provides:

Employees shall be held accountable for their conduct.
Disciplinary measures up to and including dismissal

shall be taken only for just cause. “Just cause” means that management has sufficient reasons for imposing accountability. Just cause requires: showing that the employee has committed the charged offense; offering specified due process rights specified in this chapter; and imposing a penalty appropriate to the circumstances.

The burden of proof in employee dismissal proceedings under the State merit system is well established in Delaware. The Supreme Court summarized that burden in *Avallone v. DHSS & MERB*²:

... When the State terminates a person’s employment, the MERB presumes the State did so properly. The discharged employee has the burden of proving that the termination was improper. Thus, [*the Grievant*] was required to prove the absence of “just cause,” as that term was defined in Merit Rule 12.1.

The Board concludes the Grievant failed to meet her burden to prove that she either did not make the unauthorized entries allowing a financial windfall to her coworkers, or in the alternative, that she failed to protect her PHRST identification and password pursuant to DTI policy. All unauthorized payments to CK and MR were made with the Grievant’s user identification. These payments were made over an eight-month period wherein the PHRST system requires her to change her password every 90 days. The system only allows three tries at a password before locking out the requester, and any requests to change a password requires the employee to provide her unique employee identification number. An email providing the changed password is sent directly to the email address of the requesting employee (as identified by the employee ID number). The Grievant offered no explanation as to how someone could have obtained her unique employee identification number and passwords. She specifically

² *Anthony V. Avallone v. State of Delaware, DHSS and MERB*, No. 234, 2010, (Del. Supreme, 2011) @ p. 11. <http://courts.delaware.gov/Opinions/Download.aspx?id=149750>

denied providing that information to anyone else in her office.

The Board finds the Grievant's testimony concerning the security of her password inconsistent. The Grievant claimed she never gave it out, nor did she write it down and she locked her computer every time she left her office. Yet, numerous post-it notes were taped to her desk with various passwords, including her ex-husband's social security number, to accounts including one that said "Phrst" along with an alleged password that included the name of her child, "Jaelyn26." The Grievant testified she never used that as a password in the PHRST system nor did she ever use her daughter's name as a password, in general. Yet, she later testified that at one time she did have a password to PHRST with her daughter's name.

The Board finds that there is a hole in the agency's timekeeping and payroll system as there is a period of time after the quality control review and before the closing of the records for purposes of authorizing payment which allows someone with access to the PHRST system to make changes that are not reviewed by quality control. DMS admitted this breach left their system vulnerable to actions like the one discussed in this grievance. The agency also admitted there is no way to determine the location or computer from which such a change was made and that no one looked at the entry after the quality control review.

The Board finds that the Grievant's complaint initiated the investigation that revealed the unauthorized payments and that the Grievant herself received no unauthorized payments. However, the Board finds that the Grievant, at the very least, failed to protect her access information. The Grievant knew the requirements for access and the ramifications for failure to maintain security to the PHRST system.

The Board failed to obtain a majority vote as to whether the penalty of termination was appropriate under the circumstances. While the Grievant may have failed to protect her secured access to the PHRST system (which led to financial loss to the State), she brought the situation to

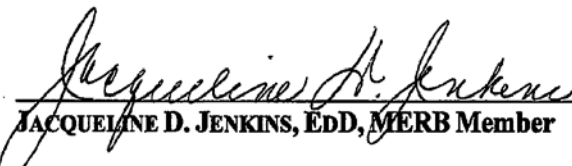
the agency's attention. There was no evidence presented on which it could be concluded that she benefited from this situation.

ORDER

It is this **3rd** day of **June**, 2016, by a vote of 2-2, the Decision and Order of the Board to neither grant nor deny the grievance; consequently the Agency's decision to terminate the Grievant stands. The Board unanimously found the Grievant committed the charged offense (violation of the Code of Conduct and IT Policies) and that the Agency provided required due process rights. The Board was not, however, able to reach a majority opinion concerning the appropriateness of the penalty of termination under the circumstances.


MARTHA K. AUSTIN, MERB Chairwoman


PAUL R. HOUCK, MERB Member


JACQUELINE D. JENKINS, EDD, MERB Member


VICTORIA D. CAIRNS, MERB Member