

Claimant was discharged for deliberate misconduct after he accessed the employer's private and proprietary business information without any justifiable basis.

**Board of Review
19 Staniford St., 4th Floor
Boston, MA 02114
Phone: 617-626-6400
Fax: 617-727-5874**

**Paul T. Fitzgerald, Esq.
Chairman
Charlene A. Stawicki, Esq.
Member
Michael J. Albano
Member**

Issue ID: 0024 4336 15

BOARD OF REVIEW DECISION

Introduction and Procedural History of this Appeal

The claimant appeals a decision by a review examiner of the Department of Unemployment Assistance (DUA) to deny unemployment benefits. We review, pursuant to our authority under G.L. c. 151A, § 41, and affirm.

The claimant was discharged from his position with the employer on January 3, 2018. He filed a claim for unemployment benefits with the DUA, which was approved in a determination issued on February 9, 2018. The employer appealed the determination to the DUA hearings department. Following a hearing on the merits attended by both parties, the review examiner overturned the agency's initial determination and denied benefits in a decision rendered on September 26, 2018. We accepted the claimant's application for review.

Benefits were denied after the review examiner determined that the claimant engaged in deliberate misconduct in wilful disregard of the employer's interest, and thus, was disqualified under G.L. c. 151A, § 25(e)(2). After considering the recorded testimony and evidence from the hearing, the review examiner's decision, and the claimant's appeal, we remanded the case to the review examiner to make subsidiary findings from the record regarding the claimant's separation from his employment. Thereafter, the review examiner issued his consolidated findings of fact. Our decision is based upon our review of the entire record.

The issue before the Board is whether the review examiner's decision, which concluded that the claimant inappropriately accessed the employer's proprietary files, for which he had no legitimate business purpose, is supported by substantial and credible evidence and is free from error of law.

Findings of Fact

The review examiner's consolidated findings of fact are set forth below in their entirety:

1. The claimant worked full-time for the employer, a CAD and Design Work Service, from November 13, 2014 to May 9, 2018 as a Senior Project Manager.

2. The employer had a policy that prohibited the employer's computers and systems to be used for personal business.
3. The claimant knew the policy, but the policy was not routinely enforced.
4. The employer had an expectation that the claimant not access proprietary files and copy/remove for personal use.
5. The purpose of the expectation was to protect assets and proprietary information.
6. The claimant's job duties did not include invoices, employment offer letters, employee payroll information, etc.
7. The claimant knew his job duties.
8. The employer's computers are networked to a central server and each employee had a login profile and access to the respective individual drive and a common drive on the server. Each computer had a hard drive on which information could be stored locally.
9. The employer does not have a dedicated IT employee and the claimant was the go-to employee for computer related issues.
10. On January 1, 2018, the Owner installed a monitoring software on the work computers which allowed the Owner to see what employees were doing. The Owner suspected that employees were using the computer for non-work-related activities excessively.
11. On January 2, 2018, at 8:09 a.m., the Owner sent an email to its employees addressing the expectation and plans for the New Year in the context of 2017 not going as planned. The Owner stated that certain policies will be enforced starting January 2, 2018 (*e.g.* computer use, lunch breaks, work schedule, *etc.*).
12. The claimant received the email and understood it.
13. From 8:12 a.m. to 9:14 a.m., at 10:06 a.m., and from 11:47a.m. to 12:04 p.m., the claimant accessed twenty-six files, all of which were located in the common drive or the claimant's hard drive.
14. The Owner, who observed the claimant's computer usage for personal matters such as using Legalzoom.com for starting one's own business, addressed the matter with the claimant before he left that morning to go to Connecticut on business.

15. When the Owner was in Connecticut and at 12:12 p.m., the claimant texted the Owner that he was going home for the day because he was not feeling well.
16. On January 3, 2018 at 6:12 a.m., the claimant texted the Owner that he was not feeling well and will not be in.
17. Later that day, the Owner sent a message to the claimant asking for his desktop password for the purpose of accessing documents needed to complete a project.
18. The claimant did not respond.
19. After getting no response from the claimant, the Owner had a friend, who worked with computers, come over and gain access to the claimant's computer, which occurred in the evening shortly after 6:00 p.m.
20. The Owner observed that the desktop was clean of icons, which he believed to be unusual.
21. The Owner viewed the recent history and observed that many files were accessed in relatively short time spans on December 28 and 29, 2017 and January 2, 2018.
22. On December 29, 2018, the claimant accessed twenty-three files located in the server file of the Owner's wife, who performed payroll, billing and other administrative duties. Some files opened were letters, invoices, bidding information, personnel information, spreadsheets, pictures, and a job offer. Other files were personal in nature.
23. One file accessed on December 29, 2017 at 9:52 p.m. contained confidential payroll and billing information.
24. At 9:55 a.m., the claimant accessed the desktop of the Owner's wife.
25. The Owner believed that the claimant removed copies of the files from the work place.
26. The Owner contacted the police and the claimant's employment terminated as a result unauthorized access to computer system and theft of files.
27. On January 22, 2018, a criminal docket was issued charging the claimant with unauthorized access to computer system and larceny from a building.

(Findings of fact ## 3, 7 and 12 added. Finding of fact # 26 modified.)

N.B. - Regarding # 7, the claimant knew his job duties and that it did not include personnel and payroll information and thus, he was reasonably aware of the expectation that such files should not be accessed. The fact that the files, particularly accessed on December 29, 2017, were not located on his portion of the server or in a public folder also suggests that the claimant should have been aware of the expectation as no expressed or implied authorization was granted by the employer. Furthermore, his behavior immediately following his access of those files support a conclusion that his conduct was nefarious in nature.

Ruling of the Board

In accordance with our statutory obligation, we review the decision made by the review examiner to determine: (1) whether the consolidated findings are supported by substantial and credible evidence; and (2) whether the review examiner's original conclusion is free from error of law. Upon such review, the Board adopts the review examiner's consolidated findings of fact and deems them to be supported by substantial and credible evidence. As discussed more fully below, we conclude that the review examiner's conclusion to deny benefits to the claimant is reasonable in relation to the evidence presented by the parties and thus supported by the record.

Because the claimant was discharged from his employment, we analyze his eligibility for benefits under G.L. c. 151A, § 25(e)(2), which provides in pertinent part as follows:

[No waiting period shall be allowed and no benefits shall be paid to an individual under this chapter] . . . (e) For the period of unemployment next ensuing . . . after the individual has left work . . . (2) by discharge shown to the satisfaction of the commissioner by substantial and credible evidence to be attributable to deliberate misconduct in wilful disregard of the employing unit's interest, or to a knowing violation of a reasonable and uniformly enforced rule or policy of the employer, provided that such violation is not shown to be as a result of the employee's incompetence

Pursuant to G.L. c. 151A, § 25(e)(2), a claimant will be disqualified from benefits if his or her separation was attributable to either a knowing violation of a reasonable and uniformly policy or deliberate misconduct in wilful disregard of the employer's interest. Under this provision, the employer bears the burden of proof.

We note at the outset that the employer presented insufficient evidence to show that the computer use policy at issue was uniformly enforced. Thus, we conclude the employer has not met its evidentiary burden under the "knowing policy violation" prong of G.L. c. 151A, § 25(e)(2). We now consider whether the employer has established that the claimant was discharged for deliberate and wilful misconduct within the meaning of this provision. As set forth below, based on our review of the entire record, we conclude that the employer has met its burden, and that the review examiner's decision is correct as a matter of law.

The employer has asserted two grounds for the claimant's separation: (1) unauthorized access by the claimant of the employer's computer system; and, (2) theft of the employers' computer files. Under Massachusetts law, "Deliberate misconduct in wilful disregard of the employer's interest

suggests intentional conduct or inaction which the employee knew was contrary to the employer's interest." Goodridge v. Dir. of Division of Employment Security, 375 Mass. 434, 436 (1978) (citations omitted). Thus, in order to determine whether an employee's actions constitute deliberate misconduct, the proper factual inquiry is to ascertain the employee's state of mind at the time of the behavior. Grise v. Dir. of Division of Employment Security, 393 Mass. 271, 275 (1984). In order to evaluate the claimant's state of mind, we must "take into account the worker's knowledge of the employer's expectation, the reasonableness of that expectation and the presence of any mitigating factors." Garfield v. Dir. of Division of Employment Security, 377 Mass. 94, 97 (1979) (citation omitted).

Consolidated Findings of Fact ## 21 – 25 establish that the claimant accessed certain files and that the owner believed that he copied and removed them from the employer's computer. While the owner's belief may be reasonable, it is not substantial evidence demonstrating that the files were actually copied and removed. Therefore, we conclude that the employer has failed to establish that the claimant engaged in theft of their computer files.

However, the consolidated findings support the conclusion that the claimant accessed personnel and payroll information, as well as personal and proprietary information, despite the claimant's awareness that the owner's policy prohibited the use of the employer's computers and systems for such purposes. Based on this policy, the owner expected that the claimant would not access the owner's assets and proprietary information. The claimant was also aware of this reasonable expectation. On December 29, 2017, the claimant accessed twenty-three files on the server of the owner's wife, whose duties included payroll, billing and other administrative duties. The claimant's job duties did not include performing billing, hiring and payroll functions. Consequently, the claimant's job duties did not require accessing the employer's confidential employee payroll and billing information, and correspondence or the personnel information, photos, or files of the owner's wife. The claimant also accessed additional files on December 28, 2017, and January 2, 2018. Based on the owner's suspicion that employees were using the employer's computer excessively for personal business, he installed a monitoring software device on January 1, 2018, which allowed him to view his employees' computer activity. The owner also saw that the claimant had used his computer for his own personal business, including accessing a legal website for starting one's own business. The claimant was terminated on January 3, 2018.

In rendering his consolidated findings, the review examiner included a note expanding on his findings. In this note, the review examiner concludes that the claimant's knowledge of his own job duties and of the employer's expectations combined with the nature and location of the files he accessed, suggests the claimant knew he should not have accessed the files in question. The review examiner also concludes that the claimant's behavior after he accessed these file indicates the claimant knew he had acted in a wrongful manner. Thus, the findings before us establish that the claimant accessed proprietary and personal computer files of the employer without authority or a legitimate business purpose for so doing. The findings further establish the claimant was aware that in accessing these files, he was acting contrary to the employer's policy and expectation regarding the use of its computers.

Therefore, we conclude as a matter of law that the claimant was discharged for deliberate misconduct in wilful disregard of the employer's interest within the meaning of G.L. c. 151A, §

25(e)(2), when he wrongfully accessed the employer's private, proprietary and personal files without any justifiable reason.

The review examiner's decision is affirmed. The claimant is denied benefits from January 21, 2018, and for subsequent weeks, until such time as he has had at least eight weeks of work and has earned an amount equivalent to or in excess of eight times his weekly benefit amount



Paul T. Fitzgerald, Esq.
Chairman

BOSTON, MASSACHUSETTS
DATE OF DECISION - February 27, 2019



Charlene A. Stawicki, Esq.
Member

Member Michael J. Albano did not participate in this decision.

**ANY FURTHER APPEAL WOULD BE TO A MASSACHUSETTS STATE DISTRICT
COURT OR TO THE BOSTON MUNICIPAL COURT
(See Section 42, Chapter 151A, General Laws Enclosed)**

The last day to appeal this decision to a Massachusetts District Court is thirty days from the mail date on the first page of this decision. If that thirtieth day falls on a Saturday, Sunday, or legal holiday, the last day to appeal this decision is the business day next following the thirtieth day.

To locate the nearest Massachusetts District Court, see:
www.mass.gov/courts/court-info/courthouses

Please be advised that fees for services rendered by an attorney or agent to a claimant in connection with an appeal to the Board of Review are not payable unless submitted to the Board of Review for approval, under G.L. c. 151A, § 37.

SPE/rh