

Employer’s circumstantial evidence did not rise to substantial evidence that the claimant engaged in the misconduct for which she was fired. There was plenty of evidence in the record indicating someone besides the claimant could have accessed the high-profile accounts from her workstation. Board rejected the review examiner’s finding of misconduct, because it was based upon a credibility assessment that failed to weigh this other material evidence. Therefore, claimant was eligible for benefits under G.L. c. 151A, § 25(e)(2).

**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: 0029 6022 98

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 reverse.

The claimant was discharged from her position with the employer on February 12, 2019. She filed a claim for unemployment benefits with the DUA, which was denied in a determination issued on March 26, 2019. The claimant appealed the determination to the DUA hearings department. Following a hearing on the merits attended by both parties, the review examiner affirmed the agency’s initial determination and denied benefits in a decision rendered on May 21, 2019. We accepted the claimant’s application for review.

Benefits were denied after the review examiner determined that the claimant had engaged in deliberate misconduct in wilful disregard of the employer’s interest and, thus, she was disqualified under G.L. c. 151A, § 25(e)(2). Our decision is based upon our review of the entire record, including the recorded testimony and evidence from the hearing, the review examiner’s decision, and the claimant’s appeal.

The issue before the Board is whether the review examiner’s decision, which concluded that the claimant had accessed the files of two high-profile patients without authorization, is supported by substantial and credible evidence and is free from error of law.

Findings of Fact

The review examiner’s findings of fact and credibility assessment are set forth below in their entirety:

1. From March 9, 2015 until February 11, 2019, the claimant worked as a full-time (40 hours per week) collections representative for the employer, a hospital and physicians network.
2. The employer maintained a Policy for Sanctions Addressing Information Security and Privacy Violations (the policy) in order to protect its patients' safety and confidentiality. The policy read, in relevant part, "Violations or breaches of information security and privacy are grounds for corrective action up to and including termination of IT privileges, staff appointment or employment. [. . .] Deliberate or purposeful violation without harmful intent. This is an intentional violation due to curiosity, convenience or desire to gain information for personal use. Examples of this type of incident include: Accessing, or attempting to access, or using PHI ("Personal Health Information") without a legitimate business need to do so or in violation of applicable policies, standards or procedures including: Accessing the information of high profile patients, coworkers, friends, family members and others."
3. At her time of hire, the claimant underwent training regarding the policy.
4. On January 7, 2019, the claimant signed the employer's annual confidentiality statement review (the review). The review read, in relevant part, "Access to confidential information without a patient care/business need-to-know in order to perform my job – whether or not that information is inappropriately shared – is a violation of this policy. [. . .] I agree to log off a [the employer] workstation prior to leaving it unattended. I know that if I do not log off a computer and someone else accesses confidential information while the computer is logged on with my password, I am responsible for the information that is accessed."
5. The claimant was aware, after having received both the policy and the review, that the employer expected her to refrain from accessing the records of patients which had not been assigned to her.
6. The claimant had access to the employer's patient database ("the system") with her unique username and password.
7. The claimant kept a notebook at her workstation with all her usernames and passwords. The claimant generally did not keep the notebook under lock or otherwise secure it.
8. Throughout her employment, the claimant, assisted several of her co-workers at her workstation with system issues.
9. On or shortly before January 23, 2019, the claimant, while watching the news, saw one of her neighbors (the neighbor) being arrested by the police.

10. As a result of having been on the news, the neighbor was determined to be a high-profile patient.
11. On January 23, 2019, the claimant worked between 7:30 a.m. and 4 p.m.
12. On January 23, 2019, between 9 a.m. and 11 a.m., the claimant conducted a training of several employees at her workstation.
13. On January 23, 2019, the employer's senior manager (the manager) took her lunch break between 12:30 p.m. and 1:30 p.m.
14. On January 23, 2019, the claimant took her lunch break between 1 p.m. and 2 p.m.
15. On January 23, 2019, at 2:14 p.m. and 3:46 p.m., the claimant logged onto the system at her workstation, using her unique username and password, and, for unknown reasons, accessed without authorization the files of the neighbor and another high-profile patient, neither of which had been assigned to her.
16. The manager, who could see the claimant's workstation from her desk, did not see anyone other than the claimant at the claimant's workstation during the afternoon of January 23, 2019.
17. On January 24, 2019, the employer's privacy team conducted an audit of the employer's high-profile patients and discovered that the claimant's username and password had been used to access the files of two high profile patients on January 23, 2019.
18. On February 6, 2019, after having been alerted of the audit's results and having viewed the report herself, the employer's human resources business partner (the HR partner) met with the claimant and confronted her with the unauthorized access. The claimant denied accessing the files of the two high-profile patients, but admitted that she recognized the name of the neighbor as someone who lived across the street from her. The claimant also told the HR partner that she keeps a notebook at her workstation with all of her usernames and passwords, and that someone else could have sat at her workstation, looked at the notebook, and accessed the system using her credentials.
19. The HR partner, concluding that the claimant had violated the employer's policies and expectations by accessing, without authorization, the files of two high-profile patients which had not been assigned to her on January 23, 2019, decided to discharge the claimant.
20. On February 12, 2019, the HR partner discharged the claimant from her employment effective immediately.

21. On February 11, 2019, the claimant filed a claim for unemployment benefits with an effective date of February 10, 2019.

[Credibility Assessment:¹]

During the hearing, the claimant denied accessing the files of the two high-profile patients on January 23, 2019. The claimant — who could not recall her work activities on the afternoon at issue — speculated that, because she kept a notebook at her workstation with all her usernames and passwords, anyone could have accessed the system, at her workstation, using her unique username. Other than vague and unsubstantiated speculation, however, the claimant did not proffer any evidence of this. Furthermore, the manager, who was present at work at the times in which the unauthorized access took place, and who could see the claimant's workstation from her own desk, testified to not seeing anyone other than the claimant at the claimant's workstation on that afternoon. Moreover, where the claimant confirmed to living across the street from the neighbor and being aware of his arrest — which would provide her with motivation to access his file — it is concluded that, based on the totality of the evidence, it is more likely that the claimant herself, using her own username and password at her own workstation, accessed the unauthorized files rather than this being an employee's elaborate plan to get her in trouble. As such, it is concluded that the claimant did, indeed, engage in the conduct that led to her discharge.

Ruling of the Board

In accordance with our statutory obligation, we review the decision made by the review examiner to determine: (1) whether the findings are supported by substantial and credible evidence; and (2) whether the review examiner's conclusion is free from error of law. After such review, the Board adopts the review examiner's findings of fact except as follows. For reasons discussed more fully below, we reject Finding of Fact # 15, because it is not supported by substantial evidence. We also note that Finding of Fact # 21 has the claimant filing her claim for unemployment benefits on February 11, 2019, the day before she was discharged. *See* Finding of Fact # 20.² In adopting the remaining findings, we deem them to be supported by substantial and credible evidence. However, we reject the review examiner's legal conclusion that the claimant is ineligible for benefits.

Because the claimant was terminated from her employment, her qualification for benefits is governed by 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

¹ We have copied and placed here the portion of the Conclusions & Reasoning section in the review examiner's decision, which explains his basis for rejecting the claimant's testimony.

² This sequence of dates, however, is not material to our decision.

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

“[T]he grounds for disqualification in § 25(e)(2) are considered to be exceptions or defenses to an eligible employee's right to benefits, and the burdens of production and persuasion rest with the employer.” Still v. Comm'r of Department of Employment and Training, 423 Mass. 805, 809 (1996) (citations omitted).

As a threshold matter, the employer must prove that the claimant engaged in the misconduct for which she was discharged. Finding of Fact # 19 states that the HR partner decided to discharge the claimant, because she concluded that the claimant had accessed without authorization the files of two high-profile patients on January 23, 2019. While there is no dispute that two high-profile patient files were accessed from the claimant's workstation on January 23, 2019, the claimant adamantly denied that she was the person who did it. *See* Finding of Fact # 18. In rendering Finding of Fact # 15, which states that it was the claimant who accessed these two patient files at 2:14 p.m. and 3:46 p.m. on that date, the review examiner determined that the claimant's testimony was not credible.

Such assessments are within the scope of the fact finder's role and unless they are unreasonable in relation to the evidence presented, they will not be disturbed on appeal. *See School Committee of Brockton v. Massachusetts Commission Against Discrimination*, 423 Mass. 7, 15 (1996). “The test is whether the finding is supported by “substantial evidence.” Lycurgus v. Dir. of Division of Employment Security, 391 Mass. 623, 627 (1984) (citations omitted.) “Substantial evidence is ‘such evidence as a reasonable mind might accept as adequate to support a conclusion,’ taking ‘into account whatever in the record detracts from its weight.’” *Id.* at 627–628, *quoting New Boston Garden Corp. v. Board of Assessors of Boston*, 383 Mass. 456, 466 (1981) (further citations omitted). Based upon the record before us, we cannot accept Finding of Fact # 15.

The review examiner's credibility assessment states three reasons for rejecting the claimant's assertion of innocence. First, he states that the claimant offered nothing beyond vague and unsubstantiated speculation that someone else did it. This improperly shifts the burden of proof onto the claimant. It further imposes upon her the obligation to prove a negative, which is very difficult. Nonetheless, the claimant apparently had tried to find such evidence. During the hearing, the employer's HR partner conceded that, upon being accused, the claimant asked her to look at the employer's video camera tapes, which may have shown the claimant going to the restroom or going to the elevators at the times that she is accused of accessing the files. The review examiner asked the employer to produce this video evidence at the continued hearing. However, the employer could not. Upon further questioning, the HR partner admitted that she did not look at the video at the time and that this evidence was deleted after 30 days, as a matter of routine business practice.³

³ This testimony about potential video evidence, while not explicitly incorporated into the review examiner's findings, is part of the unchallenged evidence introduced at the hearing and placed in the record, and it is thus properly referred to in our decision today. *See Bleich v. Maimonides School*, 447 Mass. 38, 40 (2006); Allen of Michigan, Inc. v. Deputy Dir. of Department of Employment and Training, 64 Mass. App. Ct. 370, 371 (2005).

As a second basis for rejecting the claimant's denial, the review examiner relied upon testimony from the claimant's manager, whose desk was in proximity to the claimant's workstation. Finding of Fact # 16 states that the manager could see the claimant's workstation from her desk and did not see anyone other than the claimant there during the afternoon of January 23, 2019. A close review of the hearing transcript, however, reveals testimony that the manager did not recall anybody sitting there. She added that, if somebody would have sat there, she would have noticed. The manager further testified that she would have gone to the bathroom and gone to get coffee at some point during that afternoon. Under cross-examination, she agreed that various people were at the claimant's workstation at numerous times throughout the day. These statements suggest that the manager was not focused on the claimant's workstation at all times during the afternoon of January 23, 2019. The manager also stated that she believed that the claimant did not access the accounts. Moreover, during the hearing, the employer did not dispute the claimant's assertion that she regularly helped other staff resolve problems from her workstation, that she would leave that person alone without locking the computer to retrieve copies from the copy room, and that she could be held up for up to 10 minutes waiting in line for the copies.^{4 5} Yet, the review examiner did not address any of this evidence in the credibility assessment, even though it is evidence from which a reasonable mind might infer that there were opportunities for someone else to access the claimant's workstation unnoticed.

Third, the review examiner attributes a motive to the claimant to violate the policy simply because one of the accounts belonged to her neighbor. This is an unfair leap of logic. They were both high-profile patients. By definition, many people will know them, so the motive to look them up would not be exclusively the claimant's. There is also nothing to indicate that the claimant knew the second patient. Thus, by his reasoning, the claimant would not have had a motive to access that person's record.

Because the review examiner failed to consider evidence in the record that detracted from the weight of the employer's evidence indicating that the claimant had accessed the high-profile accounts, we reject his credibility assessment as unreasonable in relation to the evidence presented. Accordingly, we reject his key finding, Finding of Fact # 15, that the claimant was the person who accessed the high-profile accounts at 2:14 p.m. and 3:46 p.m. on January 23, 2019. Given the evidence tending to show that it could have been done by someone else, the employer's circumstantial evidence does not reach the substantial evidence threshold. It is inadequate to support Finding of Fact # 15.

We, therefore, conclude as a matter of law that the employer has failed to meet its burden to present substantial evidence that the claimant engaged in the misconduct for which she was fired. She may not be disqualified from receiving unemployment benefits pursuant to G.L. c. 151A, § 25(e)(2).

⁴ These portions of the manager's and the claimant's testimony are also part of the unchallenged evidence in the record.


⁵ At one point during the hearing, the employer's third party representative objected to the claimant's testimony that someone else accessed the records. He argued that whether or not the claimant accessed the files was not the issue, and he seemed ready to stipulate to her statement that she was not the one that did it. He argued that the employer fired the claimant for leaving her workstation and password unattended, which caused the privacy breach incident. Given the employer's direct testimony that it fired the claimant for her unauthorized access, we think the review examiner properly denied the agent's objection.

The review examiner's decision is reversed. The claimant is entitled to receive benefits for the week beginning February 10, 2019, and for subsequent weeks if otherwise eligible.



Paul T. Fitzgerald, Esq.
Chairman

BOSTON, MASSACHUSETTS
DATE OF DECISION - August 30, 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.

AB