The claimant used a manager's password without permission in order to process a customer return. As she had previously been warned against using other employees' passwords to process returns, she was discharged for deliberate misconduct in wilful disregard of the employer's interest pursuant to G.L. c. 151A, § 25(e)(2).

Board of Review
100 Cambridge Street, Suite 400
Boston, MA 02114
Phone: 617-626-6400
Fax: 617-727-5874

Charlene A. Stawicki, Esq.
Member
Michael J. Albano
Member

Issue ID: 334-FHK6-DM5L

Introduction and Procedural History of this Appeal

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

The claimant separated from her position with the employer on December 10, 2024. She filed a claim for unemployment benefits with the DUA, effective December 29, 2024, which was denied in a determination issued on February 20, 2025. The claimant appealed the determination to the DUA hearings department. Following a hearing on the merits attended only by the claimant, the review examiner overturned the agency's initial determination and awarded benefits in a decision rendered on April 16, 2025. We accepted the employer's application for review.

Benefits were awarded after the review examiner determined that the claimant had not engaged in deliberate misconduct in wilful disregard of the employer's interest or knowingly violated a reasonable and uniformly enforced rule or policy of the employer and, thus, was not 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 employer's appeal, we remanded the case to the review examiner to obtain additional evidence about the circumstances surrounding the claimant's separation. Both parties attended the remand hearing. Thereafter, the review examiner issued her 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 had not knowingly violated an employer rule or policy or acted in wilful disregard of the employer's interests because she reasonably believed it was appropriate for her to use a manager's password in order to process a return, 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 and credibility assessment are set forth below in their entirety:

1. The claimant worked as a full-time receptionist for the employer, a wholesale retail warehouse, between 12/6/2023 and 12/10/2024, when she separated.

2. The claimant's immediate supervisor was the junior assistant branch manager (assistant manager). The claimant's upper-level manager was the branch manager (manager).

3. The employer maintained an information technology policy (policy) that required employees to "maintain their passwords as confidential and must not share passwords or access coworkers' equipment or accounts without express authorization." The purpose of the policy was to "prevent unauthorized access to information."

4. The policy stated, in part, "Failure to follow the Company's policies regarding information technology may lead to disciplinary measures, up to and including termination."

5. The employer communicated the policy to the claimant when the claimant electronically signed an acknowledgement that she received the employee handbook that contained the policy on 12/6/2023.

6. The employer maintained an expectation that employees do not use other employees' passwords, and to call someone that is authorized to perform returns to process all returns.

7. The claimant understood that she needed a manager's password to be entered into the system before a return could be processed.

8. The employer communicated to the claimant that she could not use other employees' passwords in the system to process returns on multiple occasions, including verbally in the spring of 2024, and in writing when she was issued a final warning on 9/6/2024.

9. On an unknown date in the spring of 2024, the manager witnessed the claimant ask the human resource manager's [sic] (HR manager) for her password to process a return. The HR manager provided the claimant with the password, and the claimant processed the return using the HR manager's password.

10. The manager verbally informed the claimant and the HR manager that they could not do that again because it was against the employer's policy. The manager stated that if it happened again, he would have to "hold [them] accountable."

11. The HR manager changed her password after the manager instructed the claimant and the HR manager that it was against the employer's policy to share passwords.

12. On 9/6/2024, the employer issued the claimant a final warning for using the HR manager's password. The final warning stated, "This is a final warning if this happens again it will lead to termination."

13. The claimant refused to sign, and she did not read the final warning on 9/6/2024.

14. On an unknown date in early December 2024, the claimant was working with a customer that wanted to return merchandise.

15. The claimant did not request that a manager provide her with their password before she could process the return. The claimant did not receive assistance from a manager to process the return.

16. The claimant used the HR manager's password to process the customer's return.

17. The HR manager did not provide the claimant with her password. The HR manager did not give the claimant consent to use her password.

18. The claimant typed in one (1) number to the register and the rest of the HR manager's password generated.

19. On 12/7/2024, the manager was performing a normal review of the employer's front end surveillance camera footage.

20. In the video footage of the front end on an unknown date between 12/1/2024 and 12/7/2024 (the final incident), the manager witnessed the claimant processing a return without requesting a manager's assistance.

21. The manager did not see the HR manager around the claimant when the claimant processed the return during the final incident.

22. The manager confirmed that the claimant processed the return using the HR manager's password during the final incident.

23. On 12/10/2024, the manager informed the claimant that she was terminated because she used another employee's password.

24. The claimant provided written responses to the Department of Unemployment Assistance's (DUA) request for fact-finding.

25. The employer provided written responses to the DUA's request for fact-finding. On the factfinding questionnaire (Questionnaire), the employer stated that the claimant was discharged for "repeated willful misconduct. Claimant's actions were within control."

26. On 1/23/2025, the employer's agent submitted a letter that provide [sic] "additional information regarding the claimant's employment and separation."

Credibility Assessment:

The parties did not dispute that the claimant was discharged on 12/10/2024 because she violated the employer's policy that prohibited employees from using or having access to other employees' passwords. It was further undisputed that the claimant used the HR manager's password to process a return on an unknown date in early December 2024, which was the final incident that led to her discharge.

Although the parties initially disputed whether the claimant received disciplinary actions about violating the policy before the final incident in December 2024, during the remand hearing the claimant admitted that she was verbally spoken to by the manager about the policy and that she received a separate written warning about the policy before she was discharged. While the claimant did not consider the verbal conversation with the manager a warning, she did not dispute that the manager verbally informed her and HR manager that they could not share passwords and/or that sharing passwords was against the employer's policy. As such, the manager's testimony that he issued the claimant a verbal warning in the spring of 2024 about improperly using the HR manager's password is found to be credible.

Likewise, the claimant's initial testimony that she did not receive a written warning in September 2024 for violating the policy is not credible based on the testimony provided at the remand hearing. After the manager testified at the remand hearing that the claimant was issued a written warning on 9/4/2024 because she violated the policy, the claimant confirmed that she was presented with a written warning that she refused to sign and she did not read. The claimant's failure to read the written warning dated 9/4/2024 does not mean it does not exist and that it was not issued to the claimant. The manager's testimony and evidence that the claimant was issued a final written warning on 9/4/2024 that stated, in part, "if this happens again it will lead to termination" is more credible than the claimant's initial testimony.

Despite the claimant's initial contention that the employer did not communicate the expectation to her, and that she did not know that she could not use other employees' passwords, the evidence and testimony at the remand hearing established that the employer communicated the expectation to the claimant through the policy, when she received the verbal warning, and when she received the final warning on 9/4/2024.

The parties disputed whether the HR manager provided the claimant with her password and/or whether the HR manager gave the claimant permission to use the HR manager's password to process the return in December 2024. Based on the manager's consistent direct testimony about the observations he made when he viewed the employer's video footage, and the claimant's repeated inconsistencies throughout her testimony, the manager's testimony that the claimant used the HR manager's password without the HR manager being present and without receiving permission from the HR manager is credible.

Ruling of the Board

In accordance with our statutory obligation, we review the record and 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 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. We further believe that the review examiner's credibility assessment is reasonable in relation to the evidence presented. However, as discussed more fully below, we reject the review examiner's legal conclusion that the claimant is entitled to benefits.

Because the claimant was discharged from her employment, her eligibility 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 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).

While the employer maintains a policy prohibiting employees from sharing passwords or accessing other employees' accounts without express authorization, it retains discretion over how to discipline employees who violate that policy. Consolidated Findings ## 3 and 4. As the employer did not provide evidence showing it discharged all other employees who accessed other employees' accounts without authorization under similar circumstances, it has not met its burden to show a knowing violation of a reasonable and *uniformly enforced* policy.

We next consider whether the employer has met its burden to show the claimant engaged in deliberate misconduct in wilful disregard of the employer's interest. To meet its burden, the employer must first show the claimant engaged in the misconduct for which she was discharged.

In this case, the employer discharged the claimant because she used another employee's password. Consolidated Findings ## 16 and 23. Inasmuch as the claimant conceded that she used the HR manager's password to process a customer return, there was no dispute that she engaged in the misconduct for which she was discharged. Consolidated Findings ## 14 and 16. Further, her decision to use the HR manager's password was self-evidently deliberate. *See* Consolidated Findings ## 17 and 18.

However, the Supreme Judicial Court (SJC) has stated, "Deliberate misconduct alone is not enough. Such misconduct must also be in 'wilful disregard' of the employer's interest. In order to determine whether an employee's actions were in wilful disregard of the employer's interest, 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). 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).

Following remand, the review examiner rejected as not credible the claimant's assertions that she was unaware that the employer expected her not to use other employees' passwords, and that the HR manager was present when the claimant had used her password to process a return in early December 2024. *See* Consolidated Findings ## 6–8. 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). Because the claimant altered her testimony substantially when she ultimately confirmed that the manager had, on two separate occasions, informed her that employees were not allowed to use other employees' passwords, we have accepted the review examiner's credibility assessment as being supported by a reasonable view of the evidence. *See* Consolidated Findings ## 8, 10, and 12.

Despite having received two previous warnings, the claimant once again utilized the HR manager's password without authorization in order to process a customer's return. Consolidated Findings ## 14–17. Pursuant to the review examiner's credibility assessment, the claimant understood that her decision to process the customer's return using the HR manager's password without authorization was contrary to the employer's expectations.

The employer's expectations around password security are facially reasonable, as they serve to protect both the employer and its employees from unauthorized access to sensitive information. *See* Consolidated Findings ## 3 and 6.

Finally, we consider whether the claimant presented mitigating circumstances for her behavior. Mitigating circumstances include factors that cause the misconduct and over which a claimant may have little or no control. *See* Shepherd v. Dir. of Division of Employment Security, 399 Mass. 737, 740 (1987). Although the claimant may have been exercising kindness by processing the customer's return, she did not show that circumstances beyond her control compelled her to use the HR manager's password to complete the transaction. Thus, the claimant has not shown mitigating circumstances for her behavior.

We, therefore, conclude as a matter of law that the claimant was discharged for deliberate misconduct in wilful disregard of the employer's interest under G.L. c. 151A, § 25(e)(2).

The review examiner's decision is reversed. The claimant is denied benefits for the week of December 29, 2024, and for subsequent weeks, until such time as she has had at least eight weeks of work and has earned an amount equivalent to or in excess of eight times her weekly benefit amount.

BOSTON, MASSACHUSETTS
DATE OF DECISION - October 21, 2025

Charlene A. Stawicki, Esq.
Member

Michael J. Albano
Member

ANY FURTHER APPEAL WOULD BE TO A MASSACHUSETTS STATE DISTRICT 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.

LSW/rh