EO: 200
BYE: 201730

State of Oregon
Employment Appeals Board
875 Union St. N.E.
Salem, OR 97311

633
DS 005.00

EMPLOYMENT APPEALS BOARD DECISION
2016-EAB-1287

Reversed
No Disqualification

PROCEDURAL HISTORY: On September 22, 2016, the Oregon Employment Department (the Department) served notice of an administrative decision concluding the employer discharged claimant for misconduct (decision # 82758). Claimant filed a timely request for hearing. On October 26, 2016, ALJ McGorrin conducted a hearing, and on October 27, 2016 issued Hearing Decision 16-UI-70031, affirming the Department's decision. On November 16, 2016, claimant filed an application for review with the Employment Appeals Board (EAB).

Claimant submitted a written argument to EAB that contained much information not presented during the hearing. OAR 471-041-0090 (October 29, 2006) allows EAB to consider information not presented during the hearing if the party offering that information shows that factors or circumstances beyond the party's reasonable control prevented it from presenting that information at hearing. However, claimant did not explain why she did not offer the information she now seeks to present during the hearing or suggest that some factor or circumstance hindered her from doing so. For this reason, EAB did not consider the new information contained in claimant's written argument. EAB considered only information received into evidence during the hearing when reaching this decision.

FINDINGS OF FACT: (1) Curry Public Transit employed claimant from March 16, 2015 until August 1, 2016, last as controller.

(2) The employer expected claimant as controller to enter accurate financial information in Quickbooks, the employer's accounting software, and to maintain accurate financial and accounting records. The employer also expected claimant to follow the instructions of supervisors. Claimant understood the employer's expectations.

(3) Sometime before approximately June 2016, claimant observed that some entries she had made in QuickBooks had been altered. Entries could be made in Quickbooks only by someone accessing that program using claimant's user identification and password. Although the general manager was able to access QuickBooks under her own user identification and password, that access was a "read only" access and she could not make or change any entries in QuickBooks. No other employees had user

identifications and passwords that allowed them to access QuickBooks. Claimant corrected the altered entries and told the general manager of the alterations she had discovered in approximately mid-June 2016. Claimant and the general manager speculated that the employer's recent upgrade to a Windows 10 operating system might possibly have corrupted the entries in QuickBooks and caused what appeared to have been alterations. Sometime later, claimant observed more alterations to QuickBooks entries she had made after mid-June 2016. Claimant also observed that entries she had made in QuickBooks for certain checks the employer had issued to federal and state taxing authorities had been deleted and accounting documents she had generated from the information in QuickBooks were altered. Claimant corrected the QuickBooks entries, and generated new balance sheets and financial statements based on accurate information.

(4) After mid-June 2016, claimant was increasingly concerned about the integrity of the employer's accounting information contained in the QuickBooks entries and the accuracy of the financial and accounting reports that were generated based on it. Claimant investigated the access history in QuickBooks in an attempt to determine who had might have altered the QuickBooks entries since she was the only person who had a QuickBooks password that would allow the making or altering of entries. The access history claimant reviewed showed that the changes to QuickBooks had been effected using her name and her password. Claimant was aware the general manager knew her password and suspected the general manager might have intentionally or inadvertently made the alterations to the information contained in QuickBooks. To protect the integrity and accuracy of the employer's QuickBooks information, claimant changed the user name and password that allowed her to access and make entries in QuickBooks. Claimant also changed the password that unlocked her computer for use. Claimant did not record the new user names and passwords in the employer's file that listed the names and passwords used by all employees. After claimant made these changes, all alterations to and irregularities in the QuickBooks information stopped appearing. Transcript at 41.

(5) In approximately early July 2016, claimant noticed that her desk had been "riffled" and the June 2016 bank and payroll files were missing. Transcript at 40. Claimant told the general manager about the missing files and the general manager told claimant she had removed them and taken them offsite to the district manager for the district manager's review. Because it was unusual for files to be removed from the employer's premises, claimant became concerned about the general manager's behavior and more concerned about the integrity of the employer's financial and accounting information.

(6) On Saturday, July 9, 2016, the general manager wanted to prepare some budgeting reports over that weekend and needed to access the employer's QuickBooks program for information. When the general manager tried to open the QuickBooks program using her own computer, user name and password for "read only access," she was not able to do so. For some unknown reason(s), the QuickBooks program had opened up for administrative access and the general manager's password would not allow her to login under that access. The general manager did not notice that she was attempting to gain administrative access to QuickBooks. The general manager then went to claimant's computer, but she was unable to unlock claimant's computer. The general manager consulted the employer's file of all passwords, but still was unable to unlock claimant's computer using the password listed in it for claimant's computer. The general manager then left a voicemail message for claimant at her home outlining her problem accessing QuickBooks. Claimant responded to the general manager's message sometime later, stating that she had not changed the general manager's password. Claimant thought the general manager's message had inquired about any changes she had made to the general manager's

password and not about any changes she might have made to her own user names or passwords. On Sunday, July 10, 2016, the general manager again went to the workplace. The general manager was still not able to access the QuickBooks program using her own password and could not unlock claimant's computer.

(7) On Monday, July 11, 2016, the general manager was able to access the QuickBooks information she needed using her own password on her own computer. Later that day, the general manager met with claimant. The Board president was present during their meeting. The general manager told claimant that she wanted all of claimant's user names and passwords, including to unlock her computer and to access QuickBooks and all other of the employer's programs. Claimant refused, stating that she was concerned that someone had been altering the information in QuickBooks, she was responsible for the accuracy of that information, she wanted to safeguard its integrity and she did not want her work to be "sabotaged." Transcript at 14. Claimant told the Board president that the general manager's "read only" access to QuickBooks, which was now allowing her access, was sufficient for all purposes for which she needed the QuickBooks information. At that juncture the meeting ended. After the meeting, the general manager tried the password she had unsuccessfully used over the weekend to unlock claimant's computer and it worked. After claimant left the meeting, the general manager went to claimant's office and told claimant she did not want claimant's password after all. Transcript at 35. Claimant thought the Board president must have been persuaded by what she had stated about the irregularities she had discovered in the QuickBooks entries, and had told the general manager not to insist on obtaining claimant's password to QuickBooks so that the information in the program would be protected from further alterations. Transcript at 35.

(8) From July 11, 2016 through August 1, 2016, neither the general manager nor any other employer representative asked claimant to provide her password to QuickBooks or any other computer programs. Transcript at 11, 48.

(9) On August 1, 2016, the employer discharged claimant for insubordination by refusing to disclose her user identification and password to QuickBooks on July 11, 2016 and afterward. At the time of claimant's discharge, the general manager told claimant that she should give her passwords to the Board president or another Board member. Claimant gave her user identifications and passwords to the Board president after she was discharged.

CONCLUSIONS AND REASONS: The employer discharged claimant but not for misconduct.

ORS 657.176(2)(a) requires a disqualification from unemployment insurance benefits if the employer discharged claimant for misconduct connected with work. OAR 471-030-0038(3)(a) (August 3, 2011) defines misconduct, in relevant part, as a willful or wantonly negligent violation of the standards of behavior which an employer has the right to expect of an employee, or an act or series of actions that amount to a willful or wantonly negligent disregard of an employer's interest. The employer carries the burden to show claimant's misconduct by a preponderance of the evidence. *Babcock v. Employment Division*, 25 Or App 661, 550 P2d 1233 (1976).

In Hearing Decision 16-UI-70031, the ALJ concluded that it was misconduct for claimant to refuse to provide her password to the general manager on July 11, 2016 or afterwards. The ALJ reasoned that claimant's stated reason for not providing the password, that she feared further tampering with the

employer's financial information in QuickBooks, was "not valid" and not a "credible basis" for refusing. Hearing Decision 16-UI-70031 at 4. We disagree.

The employer did not rebut, and appeared to concede, that someone had been making unauthorized and perhaps inadvertent, entries in its QuickBooks program, using claimant's user name and password, and that it was ongoing until claimant changed her password shortly before July 11, 2016. Transcript at 14, 21. The employer also agreed that claimant was responsible for keeping accurate financial records and that claimant likely refused to disclose her new password on July 11, 2016 because she was concerned about maintaining the integrity of the employer's financial records and preventing further alterations to the entries in QuickBooks, whether intentional or inadvertent. Transcript at 28, 49. While the employer's witness testified that the employer discharged claimant for "insubordination" when she did not provide her password, it did not show that claimant was acting to defy the authority of the general manager when she refused. Transcript at 7. The employer did not dispute claimant's explanation or that she was acting to protect the integrity of the employer's records when she refused to reveal her new password to the general manager on July 11, 2016. After the July 11, 2016 meeting, the employer did not dispute that the general manager told claimant she did not want the password after all and presumably was not going to continue insist that claimant provide it. Transcript at 35. Indeed, the general manager agreed that she did not ask claimant to provide her passwords after July 11, 2016 and through the date claimant was discharged on August 1, 2016, which was approximately three weeks later. By taking these actions and not specifically instructing claimant in response to her explanation that she was required to disclose her new password, claimant reasonably inferred the employer had accepted her stated concerns on July 11, 2016 and, on reflection, did not consider her failure to provide the new password a violation of its expectations or an insubordinate attempt to defy the general manager's authority. On this record, the employer did not show that claimant insubordinately refused to reveal her new password to the general manager on July 11, 2016, or that claimant knew or should have known the employer rejected the grounds on which based her July 11, 2016 refusal, and would consider a failure to disclose the password as an act in defiance of the general manager's authority.

The employer did not meet its burden to show claimant engaged in misconduct by refusing to disclose her new password. Claimant is not disqualified from receiving unemployment insurance benefits.

DECISION: Hearing Decision 16-UI-70031 is set aside, as outlined above.

J. S. Cromwell and D. P. Hettle;
Susan Rossiter, not participating.

DATE of Service: <u>December 14, 2016</u>

NOTE: This decision reverses a hearing decision that denied benefits. Please note that payment of any benefits owed may take from several days to two weeks for the Department to complete.

NOTE: You may appeal this decision by filing a Petition for Judicial Review with the Oregon Court of Appeals within 30 days of the date of service listed above. *See* ORS 657.282. For forms and information, you may write to the Oregon Court of Appeals, Records Section, 1163 State Street, Salem, Oregon 97310 or visit the Court of Appeals website at courts.oregon.gov. Once on the website, use the

'search' function to search for 'petition for judicial review employment appeals board'. A link to the forms and information will be among the search results.

Please help us improve our service by completing an online customer service survey. To complete the survey, please go to https://www.surveymonkey.com/s/5WQXNJH. If you are unable to complete the survey online and wish to have a paper copy of the survey, please contact our office.