Date: 20250610

File: 566-34-43563

Citation: 2025 FPSLREB 70

Federal Public Sector Labour Relations and Employment Board Act and *Federal Public Sector Labour Relations Act*

Before a panel of the Federal Public Sector Labour Relations and Employment Board

BETWEEN

MOHAMMED TIBILLA

Grievor

and

CANADA REVENUE AGENCY

Respondent

Indexed as
Tibilla v. Canada Revenue Agency

In the matter of an individual grievance referred to adjudication

Before: Audrey Lizotte, a panel of the Federal Public Sector Labour Relations and Employment Board

For the Grievor: Michael Cohen, counsel

For the Respondent: Mathieu Cloutier, counsel

Heard at Montreal, Quebec,
May 14 to 17, 2024,
and by videoconference,
July 5, 2024.

REASONS FOR DECISION

I. Individual grievance referred to adjudication

[1] When his employment was terminated, Mohammed Tibilla ("the grievor") held a taxpayer services agent position, classified SP-04, at the Canada Revenue Agency (CRA or "the employer").

[2] The termination letter, dated February 18, 2021, and signed by Chantal Tourigny, Director, Montreal Tax Services Office, CRA, alleged that the grievor made unauthorized accesses to his CRA taxpayer account five times and that he attempted to conceal it when he was questioned about it. The letter read as follows:

> …
>
> *The purpose of this letter is to inform you of my decision regarding your continued employment with the Canada Revenue Agency and of my decision with regard to your unauthorized accesses to your own account on April 4th, 2019, March 23rd and 24th, 2020, April 1st, 2020 and October 15th, 2020. Further to the Internal Affairs and Fraud Control Division (IAFCD) Report #02886 which was given to you on January 7th, 2021, and the disciplinary hearing held on January 13, 2021, I find that you contravened the Canada Revenue Agency's (CRA)* Code of Integrity and Professional Conduct *(Code) and the* Computer Systems and Electronic Networks Usage Directive.
>
> *As an employee of the CRA, you are expected to comply with the Code as well as all other CRA's directives/policies. You have been provided with annual reminders of your expected behaviour with respect to the Code and have acknowledged that you have reviewed the Code.*
>
> *In arriving at my decision, I have taken into consideration the circumstances presented. I have also considered aggravating factors, including the fact that the unauthorized accessed were repeated multiple times between April 2019 and October 2020. In addition, you attempted, at three different occasions, to conceal the misconduct and to deceive management by presenting unfounded and incoherent allegations. These behaviors are inacceptable and cannot be tolerated. I also considered the fact that you did not recognize the gravity of your conduct neither did you demonstrate any kind of remorse.*
>
> *Given that the bond of trust has been irrevocably broken, and in accordance with the authority delegated to me by the Commissioner under Section 51 (1) (f) of the* Canada Revenue Agency Act, *I hereby terminate your employment with the CRA for reasons of misconduct, effective immediately.*
>
> …

[*Sic* throughout]

[3] The grievor grieved that decision on February 24, 2021. The grievance was referred to adjudication on September 22, 2021, under s. 209(1)(b) of the *Federal Public Sector Labour Relations Act* (S.C. 2003, c. 22, s. 2).

[4] For the following reasons, I find that the alleged misconduct was established, that it justified imposing disciplinary action, and that the termination was not excessive in the circumstances.

II. Summary of the evidence

[5] The employer called the following six witnesses, all of whom were its employees:

- Rosaria Stockdale, who was the assistant director of the CRA's Internal Affairs and Fraud Control Division (IAFCD). She was responsible for overseeing the investigation into the grievor's alleged unauthorized accesses and his explanations;
- Ms. Tourigny;
- James Jones, who was the grievor's manager and who interviewed him about his account accesses;
- Robert Fazio, who was a technical advisor and trainer and provided training to the grievor;
- Sébastien Mongrain, who was a team leader with the CRA's national Information Technology (IT) service desk and who audited the grievor's interactions with the IT help desk; and
- Sergio Romanelli, who was the grievor's team leader as of April 4, 2019. He was called in reply evidence to rebut an element of the grievor's testimony.

[6] The grievor testified on his behalf, to establish that the events did not occur as alleged and that the disciplinary action was excessive in the circumstances.

A. For the employer

1. Ms. Stockdale

[7] Ms. Stockdale testified that as of the hearing, she had worked for the CRA for 22 years and had been in the assistant director role as of the events at issue. As part of her role, she was responsible for overseeing investigations into suspected employee

misconduct. On December 29, 2020, she issued an investigation report pertaining to the grievor. She had no pre-existing relationship with or knowledge of him.

[8] She explained that employees have access to only the CRA databases required to perform their duties. These are the CRA electronic systems relevant to this case:

- the Taxpayer Services Agent Desktop for Individuals (TSADI), which provides access to individual taxpayer information;
- the Online Taxpayer Information System (OTIS, also known as RAPID), which is older and provides access to individual taxpayer information too; and
- RQCH (the acronym was not explained), which is the offsite storage and retrieval system managed by the Iron Mountain company.

[9] To access those accounts, an employee must enter their User ID and confidential password. For added security, employees are required to change their passwords every 90 days. Taxpayer information is retrieved by using their social insurance number (SIN).

[10] On cross-examination, Ms. Stockdale could not say for certain if all the passwords used to access those CRA systems had to be changed every 90 days.

[11] The TSADI is designed to give agents access to the information required to answer taxpayer queries by automating gathering information from specified CRA systems, to facilitate the account analysis. The data available to TSADI users includes, but is not limited to, identification, income tax returns, assessments, benefits, revenue, diary entries, and correspondence.

[12] In terms of controls, the CRA has the Employee Electronic Access Form, which provides an audit log of every access that employees make to taxpayer information. Each page of the audit log identifies in columns the following relevant information:

- the User ID, which identifies the person who accessed a CRA electronic system;
- the System ID, which identifies the system that was accessed; e.g., TSADI, OTIS, etc.;
- the Screen ID, which identifies the screen that was viewed. Each screen is identified by a unique code;
- the PRI, which is the employee's personnel record identifier. Each employee is assigned a unique number, to identify them;

- the time and date of the access;
- the TP, which identifies the taxpayer whose file was viewed or the name of the person or organization that submitted the document that was viewed;
- the RC number, which is the Responsibility Centre where the employee works;
- the Account Number, which is the SIN of the account that was accessed; and
- the employee's name, which is identified by the User ID and sets out who accessed the system.

[13] Ms. Stockdale testified that the CRA has a proactive monitoring system called the Electronic Fraud Management System (EFM). It is designed to monitor all accesses. Predesigned rules apply to all transactions. When an employee makes an access that triggers one of the rules, an electronic alert is sent to the IAFCD, for review. One rule that is triggered quite often occurs when an employee accesses their account, in which case the EFM automatically alerts the IAFCD, for review.

[14] On cross-examination, Ms. Stockdale stated that the EFM has been in place since 2017 and that once the IAFCD receives an alert, it is logged in a case-management system and assigned to an investigator for review. She stated that alerts are generated in real time and are immediately entered into a caseload. However, they might not be investigated immediately, depending on the investigators' availability. She stated that alerts are received every day but that not all result in an investigation. If IAFCD examines the information and determines that it was a valid access that is not questionable, it closes the file.

[15] As an example, Ms. Stockdale explained that one of the rules that generates such an alert is triggered each time certain high-profile individuals' accounts are accessed. When that happens, a verification is made with the manager, to confirm if the access was intended. If it was, then the access is deemed valid. She stated that at no time is it considered legitimate for an employee to access their own account.

[16] The alerts indicate the rule that was triggered and the date and time that it occurred. In most cases, the EFM also provides a screen replay. This allows the IAFCD to see the very steps that the employee took when they accessed a CRA system. She explained that the screen replay is available when certain systems are accessed, such

as OTIS. When they are accessed, the EFM automatically records the employee's actions.

[17] Ms. Stockdale stated that two EFM alerts were generated for the grievor, indicating that he accessed his account on April 1 and October 15, 2020.

[18] On cross-examination, when asked why the April 1, 2020, incident was not investigated sooner, Ms. Stockdale explained that on March 16, 2020, all employees were sent home due to the COVID-19 pandemic and that only those considered essential were retained onsite at the workplace. She stated that the IAFCD was not considered essential, so its work was placed on hold until its staff members returned to the office in July 2020.

[19] At that point, it had a backlog of investigations to carry out. She stated that it continued to monitor the EFM during the lockdown but that it examined only serious or egregious misconduct cases. When asked whether an employee accessing their account is considered serious misconduct, she stated that she believes that it is.

[20] The investigation began with an audit of the grievor's accesses, retroactively to January 1, 2016. According to the audit-trail reports, he also accessed his account on April 4, 2019, and March 23 and 24, 2020, making a total of five accesses.

[21] When asked on cross-examination whether alerts were generated on April 4, 2019, and March 23 and 24, 2020, Ms. Stockdale replied that the TSADI was considered a relatively newer system and that the CRA was in the process of migrating information from OTIS to TSADI. She stated that because not all systems were mapped in the EFM, it was possible that the TSADI was mapped only afterward.

[22] Ms. Stockdale undertook to confirm whether EFM alerts had been generated on those earlier dates. An affidavit that she signed later confirmed that no alerts were generated. She explained that the EFM did not have the capacity to map and capture all systems at all times, due to continuous changes and upgrades in the CRA systems.

[23] Ms. Stockdale described the information contained in the audit logs and available screen replays for the five incidents.

Incident #1 - Access on April 4, 2019

[24] The audit log showed that the grievor's User ID was used to log in to TSADI at 11:15 a.m. and that a search was done using his SIN. The screens viewed were "identification summary" and "taxpayer information".

Incident #2 - Access on March 23, 2020

[25] The audit log showed that the grievor's User ID was used to log in to TSADI and RQCH from 8:36 to 8:50 a.m. and that a search was done using his SIN. The TSADI screens viewed were "identification summary", "taxpayer information". Also viewed were several accounting screens showing account history, balance, debits, credits, amounts owing, and refunds. The log also showed that a search was performed in RQCH and that multiple of its screens were viewed.

Incident #3 - Access on March 24, 2020

[26] The audit log showed that the grievor's User ID was used to log in to TSADI and OTIS from 8:47 to 8:52 p.m. and that a search was done using his SIN. The screens viewed were similar to the ones on March 23, as well as the "client vue menu" in OTIS.

Incident #4 - Access on April 1, 2020

[27] The audit log showed that the grievor's User ID was used to log in to TSADI and OTIS from 9:04 to 9:24 a.m. and that a search was done using his SIN. The screens viewed in OTIS were "base year balance summary", "payment inquiries", and "children information". The TSADI screens viewed were "taxpayer identification summary", "benefits for children — eligibility and payments", and "print history".

[28] Ms. Stockdale testified that the grievor also looked at payments of both federal and Alberta government benefits.

[29] Ms. Stockdale also referred to the screen replays obtained from the EFM for that date that set out the screens that were viewed. They also set out the commands that the grievor entered while performing the search. She stated that he looked at individual child benefit cheque payments dating to 1998.

Incident #5 - Access on October 15, 2020

[30] The audit log showed that the grievor's User ID was used to log in to TSADI and OTIS from 5:36 to 5:41 p.m. and that a search was done using his SIN. The TSADI

screens viewed were “taxpayer information”, “account balance”, “debits”, “credits”, “amounts owing”, and “refunds”. The OTIS screen viewed was a payment inquiry.

[31] Again, Ms. Stockdale referred to the EFM screen replays for that date, which set out the commands used while performing the search. She testified that the screens showed information on a refund that the grievor had received or would receive. She stated that the OTIS payment inquiry screen was for his T1 form and was related to his personal tax returns. It stipulated whether a payment was outstanding or a refund was due.

[32] Ms. Stockdale testified that based on the screen replays, the commands entered to access the screens included the grievor’s User ID, password, and SIN. She stated that to navigate between screens, the grievor used quick navigation keys, such as the F8 and F3 functions. She stated that sometimes, it was also possible to place the cursor over an item and press “Enter” to view it. She stated that the information viewed showed that the grievor had a refund of $4884.06. The next screen selected showed the details of the refund, the cheque number, and the run date, which was the date on which it was processed.

[33] Ms. Stockdale confirmed that screen replays were available only for the April 1 and October 15, 2020, alerts. She stated that generally, they are available only for the screens viewed in OTIS.

[34] Ms. Stockdale stated that after reviewing all the audit logs and screen replays, her team prepared a list of interview questions for the grievor, to inquire into the reasons for the accesses. The list was provided to his manager, Mr. Jones, to conduct the interview.

[35] Mr. Jones conducted the interview on October 23, 2020, at which the grievor provided some explanations. On October 27, 2020, he emailed Mr. Jones some additional information.

[36] Ms. Stockdale stated that IAFCD investigated each of the grievor’s explanations.

[37] On December 29, 2020, she issued the investigation report. It concluded that the grievor accessed his account on five times and that by doing so, he contravened the CRA’s *Code of Integrity and Professional Conduct* (“the Code”) and *Electronic Networks Usage Directive* (“the Directive”). The report provided the following:

…

On October 23, 2020, during a teleconference interview by James Jones, Manager, QRCC, Montréal TSO, in the presence of Andréanne Leblanc (note taker), Labour Relations Advisor, Human Resource Division, and Suzanne Ehrhardt, Union Representative, Union of Taxation Employees (UTE), Mohammed Tibilla reported he had been with the Canada Revenue Agency (CRA) since 2006. He worked as a taxpayer services agent and answered calls from taxpayers, during which he conducted confidentiality verifications using TSADI or the CRA's mainframe to validate the identity of the callers prior to addressing their questions. He reported that he had read and attested to the Code of Integrity and Professional Conduct within the past year, and that he was aware he was only permitted to access taxpayer information related to his duties.

When asked if he had ever accessed his own account, Mohammed Tibilla reported that he had. He explained that during training on October 15, 2020 related to capital gains, and facilitated by Robert Fazio, Senior Individual Services Agent, QRCC, Montréal TSO, there was a situation where Robert Fazio was trying to extract capital gains information. Mohammed Tibilla indicated that, as he previously had sold property that had a capital gain, he had asked Robert Fazio if he could use his own social insurance number (SIN) to look at the information on his own account. Mohammed Tibilla reported that Robert Fazio replied in the affirmative.

When asked about the accesses that he had made to his own account on March 23, 24, and April 1, 2020, Mohammed Tibilla reported that he did not remember making those accesses. He reported that, sometimes, when he entered a SIN and made a typographical error, he had accessed a wrong account before realizing it. He reported that he was certain he had not intentionally accessed his own account in March and April 2020, and that he must have done it in error. It should be noted that the IAFCD's review of the accesses that Mohammed Tibilla made to his own account in March and April 2020 revealed several accesses on each date. This does not support the explanation of the accesses being the result of a typographical error.

On October 27, 2020, Mohammed Tibilla sent an email to management where he reported that during March and April 2020, he had experienced an unusually high number of problems with the computer systems, including frequent freezes and the incapacity to register a SIN when input. He reported that in order to resolve these problems, he contacted the Information Technology (IT) Help Desk where an employee gained remote control of his workstation. To his understanding, resolution tests were performed by an IT employee in order to ensure the systems functioned normally and he indicated that he did not know how those tests were conducted. He reported that he felt that there was the possibility of an inadvertent error, or a mishap by the IT employee, during these tests, which, in turn, were reflected as

accesses made by him. He reported he felt that consideration should be given to this explanation.

The IAFCD's review of the Remedy ticket report for the period of January 1, 2019 to May 31, 2020 revealed there were no IT tickets created for Mohammed Tibilla on or around March 23, 24, or April 1, 2020 related to the types of system problems that he had described during the interview. It should also be noted that IT Help Desk employees only request an employee's user identification (user ID), not their SIN.

In his email of October 27, 2020, Mohammed Tibilla also reported that the audit trail report of his accesses showed he had accessed his account on April 4, 2019, which was not discussed during the interview on October 23, 2020. He reported that he remembered that after he had returned to QRCC from audit, he had experienced problems with his mainframe access and had contacted the IT Help Desk for assistance. He reported that he had informed his supervisor and the problem had been resolved.

The IAFCD's review of the Remedy ticket report for the period January 1, 2019 to May 31, 2020 revealed that an IT ticket was created on April 2, 2019, in which Mohammed Tibilla reported that he was not able to log on to Windows. At that time, he was informed by the IT employee that he was already logged on to another account with his password, so once he followed their instructions to reboot his system, the issue was resolved. The review also revealed that an IT ticket was created on April 4, 2019 by Mohammed Tibilla's manager, who had sent a request for changes to be made to his mainframe accesses as he had changed work positions. Again, it should be noted that IT Help Desk employees do not request an employee's SIN when an employee calls for assistance; the only information they ask for is the employee's user ID. The information gathered related to the IT tickets created on April 2 and April 4, 2019 does not appear to support Mohammed Tibilla's explanation of the situation.

Witness interview – Roberto Fazio

On October 30, 2020, during a teleconference interview by James Jones, and attended by Andréanne Leblanc (note taker), Roberto Fazio reported that Mohammed Tibilla was present at the training related to capital gains on October 15, 2020. When asked if Mohammed Tibilla had asked him if he could use his own SIN to look at the system, he replied that he had not. Robert [sic] Fazio reported that he may have misunderstood Mohammed Tibilla's question and thought that he may have asked if he could use a SIN, but he did not recall having a conversation with Mohammed Tibilla during the training about using his own SIN. This information is contrary to Mohammed Tibilla's account of the conversation between him and Roberto Fazio.

The Code of Integrity and Professional Conduct states that employees must never access any information that is not part of their official duties and assigned workload, including their own, as

> *this is an example of serious misconduct. Accessing information the Agency collects is strictly prohibited unless specifically required by the employee's work.*
>
> *The Computer Systems and Electronic Networks Usage Directive states that employees may only access CRA systems and electronic networks for the purpose of performing their authorized and assigned workload and duties. The Appendix D — Examples of unacceptable use of CRA systems and electronic networks, states that employees are not allowed to access their own taxpayer information or that of their relatives or acquaintances.*
>
> *The information gathered during this investigation determined that Mohammed Tibilla contravened the Code of Integrity and Professional Conduct and the Computer Systems and Electronic Networks Usage Directive when he made unauthorized accesses to his own account. The details of the unauthorized accesses are included in Appendix 1 — Overview of unauthorized accesses and the Description of systems and screens can be found in Appendix 2.*
>
> …

[38] Ms. Stockdale testified that she did not deem his explanation credible. In her experience, the audit logs were always correct since they were made automatically, without manual intervention. She stated that the fact that he logged in five separate times did not corroborate with his explanation that he might have accidentally made a typographical error. Further, each incident was for an extended period and involved multiple screen views. Had he made a typographical error, he would have exited the screen immediately. There are also procedures for employees to report accidents. The accesses were not reported to management. In total, stating that his accesses were errors did not lend the grievor credibility.

[39] Ms. Stockdale testified that the suggestion that someone else used his account was deemed not credible. That person would have had to know his password for each of the 5 accesses during a period of over 18 months, even though the passwords changed every 90 days. With respect to his explanation that the IT support agent could have used his SIN, Ms. Stockdale stated that those agents never ask for an employee's SIN; nor do they do any troubleshooting in the live production environment.

2. Mr. Mongrain

[40] Mr. Mongrain testified that as of the hearing, he had worked at the IT Help Desk for more than nine years. The desk's role is to be the first point of contact for all IT

incidents that CRA employees encounter. As a team leader, he managed his employees' performance and the calls' service quality, to ensure that all procedures were followed.

[41] Mr. Mongrain stated that information about calls is entered into the IT Help Desk's software, which is called Remedy. Once entered, it cannot be changed or removed. At the beginning of each call, the caller is asked to provide their User ID, name, work location, office where they are working, phone number, and the reason for the call. The IT agent will never ask for a SIN, as they have no use for it or a place in Remedy to enter it. IT agents also use software called Vocals that tracks all the calls that they receive.

[42] Mr. Mongrain stated that the IT Help Desk helps reset passwords and that it can provide a temporary one. When a temporary password is used, the system at issue immediately requests that the client create a new password. The process is to stay with the client until they confirm that they have changed their password. The software manages the passwords; the IT agents do not have access to them. When they view a screen, passwords always appear encrypted to the IT agents, who have no way to decrypt them.

[43] Mr. Mongrain stated that to access taxpayer information in the CRA's mainframe, an employee must enter their User ID and a password. If an incorrect password is entered, the user will be blocked after 3 failed attempts. The mainframe password must be changed every 90 days, and the same password cannot be used for the following 24 changed passwords. Passwords must be 8 characters long and include letters and numbers and a special character. The only special characters that can be used are the pound sign ("#"), the at ("@") symbol, or the dollar sign ("$"), and they cannot be used as the password's first or last character.

[44] With respect to accessing OTIS or TSADI, Mr. Mongrain stated that the IT Help Desk can only grant access but cannot access those systems. The IT agents do not know how those systems function.

[45] Mr. Mongrain stated that he audited the grievor's calls to the IT Help Desk.

[46] Based on the IT Help Desk's records, the grievor called it on April 2, 2019, and spoke with Greg Morris, one of Mr. Mongrain's IT agents. The call lasted from 8:40 to 8:58 a.m.

[47] According to the records, the grievor tried to login to his computer, not realizing that another account was logged in. He stated that that happened often, if many employees used the same computer. In that case, if someone did not log out, the next employee's password would not work, since they would not realize that they were trying to log in to another account. When that happened, the IT Help Desk instructed them to log off and reboot the computer, to force the previous session to close. The procedure was to wait with the client while they rebooted the computer. Once it was successful, the IT agent would indicate in Remedy that the issue had been resolved. That was done on the grievor's call.

[48] On cross-examination, Mr. Mongrain stated that another way that someone else could log in to an employee's computer is when an IT agent has to upgrade software and to do that has to connect to the client's computer using the IT agent's account. He stated that sometimes, it happens overnight, and the IT Help Desk ask employees to leave their computers on overnight so it can push updates onto the computers. He stated that a trace is left on the computer if that is done.

[49] When asked whether an employee could access another employee's account, Mr. Mongrain replied that the employees have access only to their accounts, which are based on what their positions require. No employee has access to another employee's account. Accounts are accessed using an employee's User ID and password. Accesses are tracked based on User IDs. Accesses to the CRA's electronic systems are granted on a need-to-know basis and must be authorized by a team leader or a manager, based on the required level of approval.

[50] The records also showed that a call was made on April 5, 2019. The grievor spoke with another IT agent. The call lasted from 10:14 to 10:53 a.m. Mr. Mongrain stated that based on his review of the record in Remedy, the grievor's keyboard configuration was not working properly for an unknown reason, so the IT Help Desk replaced it with the default one, and it worked normally after that.

[51] According to the records, the grievor contacted the IT Help Desk on March 26, 2020, and spoke with another IT agent. Mr. Mongrain stated that the grievor called because he was unable to log in to TSADI; however, he stated that it was a department-wide issue and that no one was able to access TSADI at that time.

[52] Mr. Mongrain testified that he extracted the records from March 30 to August 16, 2019, and that based on his review of them, nothing suggested that the grievor had been hacked. He stated that the procedure to follow in such cases is first to disable the account and advise the IT security team to initiate an investigation. If anything suggests that something might be odd with the account, it is deleted, and a new User ID is issued.

[53] Mr. Mongrain stated that none of that was done with respect to the grievor; nor was he aware of any employee's account being hacked. He stated that the CRA manages vital information and that the information's security is dealt with very seriously. The CRA has many firewalls and one of the strictest password protocols that he knows of.

[54] On cross-examination, Mr. Mongrain stated that his testimony was based only on his review of the records and that he did not discuss those calls with the IT agents who created the records. He stated that IT agents had to track everything they did to resolve an issue by entering it in Remedy. However, he was unable to confirm whether that was done. When he was told that the grievor would testify that Mr. Morris told him that his computer had been bugged, Mr. Mongrain replied that he had no information that could confirm or deny it.

[55] I note that based on the records entered into evidence, Cédric Roberge contacted the IT Help Desk on March 30, 2019, and requested that the grievor's account be modified and his configuration updated. Mr. Roberge was the grievor's team leader at that time.

3. Mr. Jones

[56] Mr. Jones testified that he has worked with the CRA since 1997. He became a manager for its Quebec Regional Contact Centre (QRCC) in 2020. Mr. Roberge was one of his team leaders and, as of the incidents at issue, the grievor reported to him.

[57] Mr. Jones first became the grievor's manager in December 2019. He stated that the grievor's hours of work were from 9:00 a.m. to 5:00 p.m. He described his relationship with the grievor as very cordial. He stated that the grievor always had a big smile and that he is friendly. He stated that before the incidents at issue came to light, he never had any problems with him.

[58] Mr. Jones stated that CRA employees are not allowed to log in to and review their accounts. When employees log in to the mainframe, three screens appear, each of which states that access is on a need-to-know basis. The assistant commissioner's and director's offices also send periodic reminders to that effect.

[59] Mr. Jones stated that he was asked to interview the grievor about the unauthorized accesses and that he was provided the questions to ask. The interview was done on October 23, 2020. Since they worked from home at that time, they met over the phone. A representative from the CRA Labour Relations team, Andréanne Leblanc, and a bargaining agent representative, Suzanne Ehrhardt, were also on the call, which was not recorded. Both he and Ms. Leblanc asked questions of the grievor, but only Ms. Leblanc took notes.

[60] During the interview, the grievor denied accessing his account other than once, on October 15, 2020, as part of training. He told Mr. Jones that he had taken capital gains training and that he asked the trainer if he could use his account, since he had recently sold some property, and that the trainer, Mr. Fazio, told him that he could use his SIN.

[61] Mr. Jones stated that he was taken aback by that statement, since Mr. Fazio was one of the most senior and competent trainers that the CRA had. He stated that he found it difficult to believe that Mr. Fazio would tell someone to use their SIN.

[62] Mr. Jones said that he sent an encrypted email to the grievor during the interview, to show him the audit logs for April 4, 2019, and March 23 and 24, April 1, and October 15, 2020, and that they we went through them together. He stated that the grievor admitted to accessing his account on October 15, 2020, but stated that he had not accessed his account, or had no recollection of it, other than on October 15. He said that perhaps he had accessed it accidentally, in error.

[63] In cross-examination, Mr. Jones was informed that the grievor denied that he was provided with an encrypted copy of the audit log. Mr. Jones replied that he sent it, and undertook to find a copy of his email confirming it. I was informed that that was done.

[64] In cross-examination, Mr. Jones was also asked for his understanding of the grievor's comment that sometimes, he entered the wrong SIN. Mr. Jones stated that he

was confused since he did not understand how a person could accidentally enter their SIN. When asked whether it was possible that he had misunderstood the grievor's explanation and that the grievor had spoken only in general terms, Mr. Jones replied that he knew what he had been told. He agreed that it was mathematically impossible for the grievor to accidentally input his SIN.

[65] Mr. Jones emailed the grievor on October 26, 2020, with the interview notes that Ms. Leblanc prepared. He confirmed that they accurately reflected the conversation during the interview. When asked in cross-examination whether they were a verbatim reproduction of what was said, Mr. Jones replied that they captured 95% of what was said.

[66] His email to the grievor stated the following:

> *Please review them and if you wish to make any changes, send them to me in a separate encrypted email before Wednesday, October 28, 2020. Once you have reviewed the document, and if there are no changes, you must initial each page before electronically signing. Once initialed and signed, return the document to me before the end of day Wednesday, October 28, 2020.*

[67] Mr. Jones referred to an email received from the grievor on October 27, 2020, in which the grievor stated this: "Attached are the initialized and signed documents as instructed. Little modification may follow in separate sheet." Another email was received from him on October 27, 2020, which provided additional information.

[68] Mr. Jones sent both documents to his assistant director. He then met with Mr. Fazio on October 30, 2020, to inquire if he recalled a conversation with the grievor in which he asked if he could use his SIN. Mr. Fazio replied that he doubted it but that if he had done so, it was because he did not understand the question.

[69] Ms. Leblanc was also in attendance and took notes of the meeting. Mr. Jones confirmed the accuracy of the notes. During cross-examination, he stated that the notes were not verbatim but that they were as close as possible. He agreed that the statement about Mr. Fazio doubting that he would have told the grievor that he could use his SIN was not recorded in the notes.

[70] The interview notes were entered into evidence. They read in part as follows:

…

> ***JJ:*** *He accessed his own account since he did not have a SIN to look at the systems. Did he ask you if he could use his own SIN? Did you say he could?*
>
> ***RFG:*** *No I did not. Maybe I did not understand the question. No, if I would have understood the question I would not have said that he could access his own account. If I did not understand I may have said he could use a SIN.*
>
> …
>
> ***AL:*** *Robert, do you recall any conversation with Mr. Tibilla or a question from Mr. Tibilla concerning a SIN or using his own SIN?*
>
> ***RFG:*** *Do not recall any conversation. Maybe I misunderstood what he said and said ok. We were looking at SINs. I would definitely not have said yes if I understood that he would have accessed his own account.*
>
> …

[71] Mr. Jones stated that he was provided with Ms. Stockdale's December 29, 2020, investigation report. He then emailed the grievor on January 7, 2021, summoning him to attend a disciplinary hearing. The email informed him that the review of the audit trail had confirmed that he had accessed his account without authorization on April 4, 2019, and March 23 and 24, April 1, and October 15, 2020. It stated, "At this stage of the process, the objective of this meeting is to gather your comments." It informed him that a decision would be rendered after the hearing and enclosed a copy of the investigation report.

[72] Mr. Jones stated that during the disciplinary hearing, the grievor continued to deny that he had accessed his account on the first four dates. As for the accesses on October 15, 2020, Mr. Jones stated that he pointed out to the grievor that some of the screens accessed had nothing to do with capital gains, however, the grievor denied accessing them. He stated that the grievor explained that maybe IT had accessed his account.

[73] Mr. Jones stated that he did not find the grievor's explanations believable. He asked the grievor whether he meant that someone had acquired access to his SIN, User ID, and passwords and that the grievor replied that it could have happened. Mr. Jones stated that the grievor's suggestion that IT could have accessed his files inadvertently did not hold water because he did not contact IT on those dates.

[74] A copy of the notes taken during the disciplinary hearing were entered into evidence. Mr. Jones confirmed that they accurately reflected the conversation.

[75] He stated that he left the meeting feeling that the grievor had been disingenuous and had invented stories just to cover himself. He did not think that the grievor had been believable. He felt that the bond of trust had been broken and that he could no longer trust the grievor. He decided to speak with his assistant director since his delegated authority for disciplinary measures was limited to a 30-day suspension. He stated that that was the end of his involvement. He was informed later that the decision had been made to terminate the grievor's employment.

[76] On cross-examination, Mr. Jones agreed that during the five unauthorized accesses, no changes were made to the files — they were only viewed. He stated that had the grievor admitted to what he had done and apologized, Mr. Jones would have recommended a 30-day suspension. He agreed that that was based on the CRA's discipline directive.

4. Mr. Fazio

[77] Mr. Fazio stated that as of the hearing, he had been working at the CRA for 20 years. In 2020, he was a senior taxpayer agent classified at the SP-05 group and level; it was a unionized position. His main role was to assist taxpayer agents with their calls and provide training and coaching. He had been doing that for 15 years.

[78] Mr. Fazio described his relationship with the grievor as "great" and stated that they had a very good rapport. He stated that he liked the grievor and that they had had some good times. He stated that he had trained the grievor twice and had coached him about 10 times.

[79] From October 5 to November 13, 2019, he provided training on capital gains and losses, trust returns, rental income, and international returns. The grievor was 1 of 15 participants. The classes were held virtually from 9:00 a.m. to 5:00 p.m. each day.

[80] He stated that at the start of each training session, he warned the class that they would see SINs and that if they knew the taxpayer who held one of the SINs, they were to immediately inform him, so that a different one could be chosen. This was because they were not allowed to look at the SIN and tax information of a person they knew.

[81] During that training, TSADI and the T1 Case system were used. OTIS was not used.

[82] He stated that OTIS is older and that it was rarely used since information such as capital gains had been removed from it. It still contained old information, such as child benefits. He stated that he is very familiar with OTIS since he used it for 20 years. He stated that keyboard function keys are used to navigate OTIS. He stated that it cannot be navigated without those keys, but that in some of its zones, using mouse clicks is possible. He stated that F3 is used to go back and that F7 and F8 are used to toggle between the screens. He stated that there was no reason to use OTIS for capital gains training.

[83] Mr. Fazio was asked to view the grievor's screen replays from October 15, 2020. He stated that none related to capital gains. He stated that there was actually no need to go into OTIS for capital gains since it contained no such information. He stated that the G1 function key that was used brought the user to a list of refunds that a taxpayer had received. Mr. Fazio stated that the next function used in the screen replays showed that the grievor looked at information about a cheque's status. The screen showed that a payment was sent on October 14, 2019. He stated that none of that information related to the capital gains training.

[84] Mr. Fazio stated that he has never authorized a student to access their account because they are not allowed to. He stated that that is taught as part of their basic training. There are also warnings in the CRA's electronic systems to remind employees that they are allowed to access it only for work purposes.

[85] When asked why he allowed the grievor to use his SIN in OTIS, Mr. Fazio replied that he did not and that he would never do that.

[86] On cross-examination, he was asked whether he recalled the interview on October 30, 2019, and stating that it was possible that he might have authorized the grievor to use his SIN, if he misunderstood the grievor's request. He replied that he recalled saying it. However, he added that he would never have said that employees could access the system using their SINs. He added this: "But I like [the grievor], we have had good times together. So I said that maybe I misunderstood his question. I have a lot of people asking me questions."

5. Ms. Tourigny

[87] Ms. Tourigny testified that she has been with the CRA since 1992. As of the events at issue, she was the director of the CRA's Montréal Tax Services Office. Her relationship with the grievor as of the events at issue was strictly professional. She never had any issues with him before then.

[88] Ms. Tourigny stated that the CRA's tax system is based on the pillars of trust, honesty, and integrity. Those fundamental core values are in everything that it does and are critical to maintaining the public trust. Their importance is highlighted in the Code and the Directive.

[89] She stated that those documents dictate employees' required behaviours. They state clearly that CRA employees have to uphold the highest conduct and that they cannot conceal any misconduct. Having access to taxpayer information is a privilege, not a right. Those documents set out examples of misconduct, including an employee accessing their information. She stated in no circumstance is an employee allowed to look at their file. Employees are reminded of that every day when they log in to their computers. It is also part of employee training and is repeated during multiple annual awareness campaigns.

[90] If an employee tries to conceal an unauthorized access, it creates a situation of mistrust and impacts the CRA's ability to maintain Canadians' trust.

[91] Ms. Tourigny stated that she was first informed of the unauthorized accesses when she received an email from the IAFCD, informing her of the investigation. Her next involvement was after the disciplinary interview. She became involved since Mr. Jones did not have the authority to terminate an employee.

[92] Before she decided to terminate the grievor, she reviewed IAFCD's investigation report, the audit logs, and the screen replays, along with the notes from the disciplinary process, the interviews, and the grievor's additional information that had been provided in an email.

[93] She stated that the decision to terminate the grievor's employment was made based on the facts that he provided unfounded allegations, lacked accountability, repeated the unauthorized accesses, lacked honesty, and blamed others. By doing those things, he disrespected the CRA's values. She stated that contact agents are the

face of the CRA and that they must be held accountable and must protect and strengthen the tax system. They may access an account only if it is part of their job.

[94] She stated that she considered the number of times that the grievor made unauthorized accesses and that he concealed his misconduct, made unfounded allegations, lacked accountability and remorse, and blamed others as aggravating factors in her decision. She also considered his position within the CRA and the real or potential damage to the CRA's integrity and the failure to protect it. She stated that concealing wrongdoing is the highest offence that a CRA employee can commit. The grievor broke the bond of trust with the CRA. That was the main reason she decided to terminate his employment.

[95] She stated that she considered his years of service since he had been working for the CRA since 2006. But she also considered the amount of training and number of warnings that he received during that time.

[96] She stated that she did not rely on any prior disciplinary action that the grievor had received.

[97] She stated that she informed the grievor of her decision during a meeting on February 18, 2021. She explained the termination to him and provided him with her signed termination letter. Ms. Leblanc took notes at that meeting, which were entered into evidence. Ms. Tourigny confirmed their accuracy.

[98] On cross-examination, she stated that the audit log showed that on March 23 and 24, April 1, and October 15, 2020, the grievor accessed information for the year "19MY". She stated that that represented multiple-year information and included capital gains, carry forward, carry back, and rental gains or losses.

[99] Still on cross-examination, she was shown information from the audit logs that indicated that more than one screen was viewed at once. She stated that that was because all the contact agents had and worked from two screens, so they could look at them both at the same time.

B. For the grievor

[100] The grievor testified that he had worked with the CRA since 2006. He held several term contracts over the years, with some service breaks. He became a permanent employee on November 1, 2020.

[101] The grievor referred to two previous grievances. The first was dated June 10, 2019, and in it, he grieved a written reprimand dated May 22, 2019, for insubordination on March 28 and 29, 2019. The second was dated December 20, 2019, in which he grieved his performance evaluation for September 1, 2018, to March 31, 2019. Both documents were entered into evidence on consent. The parties acknowledged that I was not seized of either one. The written reprimand was reduced to a verbal warning, while the performance-evaluation grievance remained outstanding.

[102] The grievor also entered into evidence a complaint of psychological harassment, differential treatment, and favouritism dated April 4, 2019 ("the harassment complaint"). It related to incidents in the workplace dating from 2018 until March 29, 2019. The employer objected to it being entered into evidence, as the grievance with which I am seized does not allege discrimination, and notice was not provided to the Canadian Human Rights Commission (CHRC), as required by the Federal Public Sector Labour Relations and Employment Board's ("the Board") legislation. The grievor's counsel argued that the document served to show the context of the events just before the first alleged breach on April 4, 2019.

[103] I allowed the harassment complaint to be entered as proof of its existence but not as proof of its content, as I am not seized of it; nor does the grievance refer to it. It highlighted workplace tensions, predominately between the grievor and his team leader at that time.

[104] Of note, the grievor's term contract ended on March 31, 2019. The events of March 29, 2019, occurred on a Friday — the last working day of his term contract. On Monday, April 1, 2019, he started a new term contract with a different unit and reported to a different manager and team leader.

[105] The grievor stated that at a point on March 29, 2019, he went to the bathroom. Before doing so, he logged out of his computer but did not close it. When he came back, he was asked to go to his supervisor's office. He was then brought to his office to

retrieve his things and was asked to go home for the rest of the day. He stated that his team leader took his computer.

[106] The grievor stated that he believed that that incident was related to his termination. He stated that when his team leader took his computer, she did not ensure that it was closed, as she should have done, based on the usual protocols, to prevent any compromises. He stated that since it was the last day of his contract, certain protocols should have been followed. He stated that at the ends of his earlier contracts, the supervisor would take his computer, ensure that all the security measures were in place, and ensure that the grievor had exited the CRA systems and logged off before taking the computer. That was not done on March 29, 2019.

[107] He stated that on April 4, 2019, Mr. Morris of the IT Help Desk informed him that his computer had been hacked. Given the closeness of the two events, and given that it had never happened to him before, he believed that that was the source of the problems that then occurred.

[108] The grievor stated that on April 4, 2019, he informed his new supervisor Mr. Romanelli that the IT Help Desk had detected that his computer had been hacked. He stated that Mr. Romanelli asked him if the issue had been resolved, and he replied that it had. He stated that he was not made aware whether there was an investigation into it afterward.

[109] The grievor stated that when he was terminated, he was working as a client service agent. His role was to receive calls transferred from the contact centre, and when that happened, he had to follow a process. He would ask for the caller's SIN number, to access their information. After he had properly identified the caller, he would inquire into the purpose of the call and try to address the reason for it. Most calls involved the T1 tax form and registered retirement savings plans.

[110] He stated that he was not able to change anything in the CRA systems and that he could only request a change and enter the information that the caller provided. That was made in TSADI. He stated that once information was entered into TSADI, it could not be changed.

[111] The grievor stated that although he had two computer screens when he worked in the office, he used only one. Once he began working from home in March 2020, he had a laptop and one computer screen.

[112] In terms of navigating the CRA's systems, the grievor stated that TSADI is simple and that a keyboard or mouse is used. OTIS is normally navigated by using function keys. He stated that he would use the up or down arrow keys to navigate between pages. He stated that he did not use the F7 function. He stated that he never used the function keys since there were so many of them. He stated that he preferred to use the arrow keys.

[113] On cross-examination, when asked whether it was possible that the only thing that the up and down arrow keys allowed was to move up and down a page but not to change pages, the grievor replied that it had been a while, so he did not really remember. He did not really use OTIS most of the time, and his testimony was what he recalled. He stated that most of the time, he would go to the page that he needed and then use the F3 function key to leave it. He agreed that he had worked for the CRA since 2006 and had used OTIS from the beginning.

[114] The grievor stated that when he initialized the interview notes that he sent to Mr. Jones, his understanding was not that he was accepting their content. He stated that Mr. Jones told him to sign them, to confirm that all the pages had been received.

[115] On cross-examination, he agreed that he was informed before and after the interview that he could make changes to the interview notes and that he understood it. He agreed that he was given time to review them, that he signed them, and that he returned them to Mr. Jones. He stated that he did not take any notes during the interview and that his testimony was based on his recollection.

[116] The grievor stated that after he read the interview notes, he noticed that the April 4, 2019, incident had been added, although he was not questioned about it during the interview. He decided to send an email to raise that issue. He stated that he wanted to alert Mr. Jones to the fact that he had been hacked on April 4, 2019, and that the CRA should investigate it. He stated that his email referred to his computer being "budded" but what he meant was "bugged".

[117] I noted during the grievor's testimony that he used the terms "bugged" and "hacked" interchangeably.

[118] On cross-examination, the grievor stated that the audit-trail log that he received during the October 23, 2020, interview was not the same one that was entered into evidence. He stated that he could not recall exactly what he had seen since it was shown to him in his words "fast-fast" and was then deleted. He stated that he was asked to look at the document, so he did. He was then asked whether he had seen it. When he replied that he had, it was then deleted. He stated that he could not describe how it was different from what he had seen since he could not recall anything about the documents that he had seen. However, he just knew that it was different from what he was shown on October 23, 2020.

[119] With respect to the interview notes, and the comments about accidentally entering a SIN, he stated that he had been talking in general terms because the conversation was about accessing the wrong account. He stated that sometimes, a SIN was mistyped, and on realizing that it was the wrong file, it was closed. He was not referring to accidentally entering his SIN.

[120] The grievor stated that he was aware of the Code and the Directive and that it was prohibited for an employee to access their account. He stated that that was why he would never have done it. He would never have accessed his account and jeopardized his employment.

[121] He stated that he had no reason to look at the child benefits information. He stated that he did not have any child or relatives that received benefits. His child was 39 years old and had stopped receiving benefits in 1996. He stated that the employer alleged that he looked at benefits for Alberta, but he had always lived in Quebec, and he did not look at any of the benefits that he was accused of having looked at.

[122] With respect to October 15, 2020, he stated that he admitted to accessing his account on that date for the reasons that he had provided. However, he stated that there was no need for him to look at the G1 screen as alleged since he already had all that information.

[123] On cross examination, the grievor agreed that the CRA runs several campaigns to remind employees that accounts can be accessed only for work purposes. He agreed

that trust, honesty, and integrity are the CRA's pillars and are an essential part of the employee-employer relationship. He stated that he understood that he had to be honest at work and during his testimony, and he recalled making an oath of office to act with integrity and honesty.

[124] On cross examination, the grievor agreed that income tax returns must be filed with the CRA by the end of April of each year. He also agreed that he received a cheque from the CRA in October 2020 for a refund that he was owed with respect to prior years' taxes. He stated that he never filed any paperwork to receive that amount.

[125] On cross examination, the grievor stated that he reached out to the IT Help Desk perhaps twice in April 2019. He was not able to recall how many times he reached out to it in March 2019. He stated that he remembered speaking with Mr. Morris from the desk on April 4, 2019. When asked whether it was possible that he had spoken with Mr. Morris on April 2, the grievor replied "No", but he stated that he had spoken to him multiple times.

[126] The grievor stated that he had not taken notes of those calls. When asked how he could recall that specific date, he stated that it was because it was important to him and that he had reported it to his supervisor. He stated that he went to his supervisor's office and spoke to him.

[127] On cross-examination, the grievor stated that he was convinced that the call with Mr. Morris occurred on April 4, 2019. He stated that he could not recall the call on April 2, 2019. He added that Mr. Morris did not tell him that his computer had been "budded" but that that is what he understood. He stated that Mr. Morris expressed surprise and said, "Oh, your account is bugged!" and then told him to close and reboot his system. After he did, Mr. Morris told him that his computer was fine. The grievor stated that he did not discuss it with anyone else from IT. He stated that he called the IT Help Desk that day because he could not access his CRA systems.

[128] On cross-examination, the grievor agreed that his password was required to enter the CRA's systems. He agreed that on October 15, 2020, he accessed his file in TSADI. He stated that he recalled doing so in the morning. He stated that he did not recall accessing the T1 Case system, and he denied accessing OTIS.

[129] The grievor was shown the notes from his disciplinary hearing on January 13, 2021, which set out that he had acknowledged that he had accessed OTIS, TSADI, and T1 Case about capital gains. When asked whether it was possible that his memory of the incident was better then than at the hearing, he stated that the notes were wrong and that he had not told Mr. Jones that he had accessed OTIS. He stated that for the training, TSADI and T1 Case were relevant but that there was nothing for him to look at in OTIS.

[130] He stated that during the interview, he was asked about the refund and replied that he had had no need to take a look in that system. He agreed that there were no links between the capital gains training and the information in OTIS. He agreed that he was provided with a copy of the interview notes and with an opportunity to amend them, but that he did not.

[131] On cross examination, when questioned about the explanation that he provided to the effect that IT employees might have inadvertently accessed his account, the grievor replied that he was not accusing them. He stated that he was answering in general terms and saying that something must have happened and that the CRA should investigate it further.

[132] The grievor asked to enter into evidence a completed CHRC form in which he alleged that he suffered discrimination on the basis of race, national or ethic origin, and colour. The form referred to the events that started on October 23, 2020, when he was interviewed for the unauthorized accesses of his account until his termination on February 18, 2021. He stated that he filed it with the CHRC. The employer objected to it on the basis that it was undated and unsigned and because the employer had never received it.

[133] On May 17, 2024, the grievor's representative undertook to obtain a signed and dated version of the form. When the hearing started on July 5, 2024, he stated that whether it had been filed remained a mystery. However, he had intended to make a complaint. The employer agreed that it be entered into evidence for proof of its existence but not of its content. I note that in it, the grievor stated the following:

…

> *I accessed my personal account on October 15th 2020 in a class room* [*sic*] *setting for learning purposes, with the permission of the*

> *class room* [*sic*] *monitor, as he could not find an account number with the related information to demonstrate to the class. This fact was made clear to the interviewer and observers during that interview.*
>
> …

C. The employer's rebuttal evidence

1. Mr. Romanelli

[134] Mr. Romanelli stated that he has been working for the CRA since 2004. From April to August 2019, he was the grievor's team leader. He stated that he had a good professional relationship with the grievor and that he did not have any issues with him.

[135] He stated that he never discussed with the grievor IT issues or the grievor's account being hacked. He stated that he never heard of any employee having their account hacked in his 20 years with the CRA.

[136] On cross-examination, he admitted that he did not recall all his conversations with the grievor in 2019.

[137] In redirect examination, he stated that he was confident that he had never discussed any issue about the grievor's account being hacked since it would have been of great magnitude and so would have been escalated to higher management and required investigation. He stated that he would have recalled a conversation of that magnitude since it was a big security issue. Had the grievor told him about an issue with his mouse, or something similar, it would have been a small thing that he would not have remembered, but an account being hacked was a high-security issue that would be remembered for years.

III. Analysis and reasons

[138] To reach a decision, it is first necessary to determine whether the employer established that misconduct occurred that justified taking disciplinary action against the grievor. If so, I next must determine whether the decision to terminate his employment was an excessive response in the circumstances and whether an alternative remedy should be substituted (see *Wm. Scott & Company Ltd. v. Canadian Food and Allied Workers Union, Local P-162*, [1977] 1 Can. L.R.B.R. 1).

[139] The employer had the burden of proof of establishing the facts on a balance of probabilities with clear, convincing, and cogent evidence (see *F.H. v. McDougall*, 2008 SCC 53 at paras. 46 to 49).

[140] As the grievor denied any wrongdoing, this case turns entirely on credibility. I relied on the following oft-cited approach in *Faryna v. Chorny*, 1951 CanLII 252 (BC CA) at 357, to assess the credibility of the evidence presented to me:

> *The credibility of interested witnesses, particularly in cases of conflict of evidence, cannot be gauged solely by the test of whether the personal demeanour of the particular witness carried conviction of the truth. The test must reasonably subject his story to an examination of its consistency with the probabilities that surround the currently existing conditions. In short, the real test of the truth of the story of a witness in such a case must be its harmony with the preponderance of the probabilities which a practical and informed person would readily recognize as reasonable in that place and in those conditions.…*

[141] The grievor also referred me to Turmel c. Conseil du Trésor (Service correctionnel du Canada), 2009 CRTFP 122; Syndicat québécois des employées et employés de service, section locale 298 (FTQ) et Centre d'hébergement Saint-Vincent-Marie (Mireille Davilmar), 2016 QCTA 396; and Syndicat des employés de métier de la Buanderie centrale de Montréal (CSN) c. Buanderie Centrale de Montréal, 2024 CanLII 18619 (QC SAT) which all stand for the essentially same proposition.

A. Was there conduct that gave rise to discipline?

[142] The employer's termination letter alleged that the grievor made unauthorized accesses to his account on April 4, 2019, and March 23 and 24, April 1, and October 15, 2020, and that he contravened the Code and the Directive. As aggravating factors, it relied on the fact that the unauthorized accesses were repeated multiple times over the span of 18 months, that 3 different times he attempted to conceal his misconduct and deceive the employer, and that he failed to show remorse or understanding of the gravity of his misconduct.

[143] Having carefully assessed the evidence, I find that the employer established that it had grounds to impose disciplinary action on the grievor. The following are my reasons.

1. The unauthorized accesses

[144] Ms. Stockdale testified that she was alerted to the unauthorized accesses when she received system-generated alerts. She explained that alerts are generated automatically when certain rules are breached. In this case, the breach concerned an access by an employee of their account, which the Code and the Directive prohibit. The grievor did not contest it. He agreed that it was prohibited and admitted to being aware of that rule throughout the relevant period.

[145] The alerts caused the IAFCD to audit the grievor's account. The audit revealed that his account had been accessed five times using his User ID and SIN. An audit log was entered into evidence that corroborated that information.

[146] The grievor admitted to accessing his account on October 15, 2020. However, he denied that he accessed all the screens shown on the audit log or at the time indicated.

[147] To agree with the grievor, I would have to determine that the CRA audit logs had been falsified to change their content, that the EFM generated faulty reports, or that someone else logged in to the CRA's systems using the grievor's User ID and SIN that same day. The evidence supported none of those conclusions.

[148] The grievor alleged that on October 15, 2020, Mr. Fazio gave him permission to access his account during the capital gains training that he was attending. He claimed that he accessed his account during the morning, and not at 5:36 p.m., as indicated in the audit log. I find that his story lacks credibility, for the following reasons.

[149] First, Mr. Fazio denied providing that permission or having any conversation with the grievor about it. While it is true that he stated that he might have misunderstood the grievor's question, I believe that that comment was motivated by his relationship with the grievor. Indeed, he stated that he had coached the grievor about 10 times and that he liked him. However, he stated very clearly that he would never have authorized such an access.

[150] Second, the interview with Mr. Fazio occurred on October 30, 2020, which was close to the date of the alleged conversation; as such, his memory was likely still relatively fresh. Had Mr. Fazio had any conversation with the grievor resembling a request to access any of the CRA system using a SIN, the probabilities favour that he would have recalled it.

[151] Third, Mr. Fazio confirmed that the screens that were viewed, as identified in the audit log, had nothing to do with the capital gains training. That weighs in favour of the accesses having been made for personal reasons and not for training purposes, as the grievor alleged.

[152] Fourth, the training took place between 9:00 a.m. and 5:00 p.m., and the audit log indicated that the access was made at 5:35 p.m. That directly contradicted the grievor's allegation that he accessed the screens during the morning, as part of the training.

[153] Fifth, the grievor had a motive for accessing his account on October 15, 2020, since he expected a large refund from the CRA. Indeed, one of the screens viewed showed that a cheque of $4884.06 had been created the day before; therefore, he was about to receive it.

[154] Sixth, the grievor claimed that he accessed his account during the morning; however, no audit log supports that claim. This weighs in favour of him having made the access in a way that was contrary to what he alleged.

[155] Seventh, the access was part of a pattern of behaviour, as the audit logs set out that he had accessed his account four times before.

[156] Eighth, everyone involved in investigating the unauthorized accesses either had a good working relationship with the grievor or had no prior knowledge of him. Therefore, no one had reason to falsify the audit log.

[157] Ninth, access to the information in the audit log required the grievor's User ID and password, as well as his SIN. He was the only one who knew his password. That weighs heavily in favour of him having accessed the CRA's systems, as indicated in the audit log.

[158] The totality of that evidence leads me to find that the grievor's account of the events of October 15, 2020, is simply not credible. As stated in *Faryna*, the test of the truth of a witness's story must be its harmony with the preponderance of the probabilities that a practical and informed person would readily recognize as reasonable in that place and in those conditions. In this case, the evidence overwhelmingly supports the determination that the grievor accessed his account on October 15, 2020, as shown in the audit log.

[159] I further determine that the employer provided clear, cogent, and compelling evidence that the grievor also accessed his account on April 4, 2019, and March 23 and 24 and April 1, 2020. I make that finding for the following reasons.

[160] Ms. Stockdale testified that the audit log showed that the grievor's User ID and SIN were used to access several CRA systems that contained taxpayer information. The audit log was entered into evidence and corroborated that his accounts were accessed on the four dates in question. She testified that in her years of experience, the audit logs have never been incorrect.

[161] Ms. Stockdale and Mr. Mongrain both stated that to access the grievor's account, as shown in the audit logs, someone had to first enter the grievor's User ID and password. Only he knew the password, which otherwise was not accessible. The password changed every 90 days, and the same one could not be used in the next 24 password changes. Since the unauthorized accesses occurred over a span of 18 months, it by necessity meant that his password changed multiple times during that period. The grievor did not challenge any of that information; nor did he testify that he shared his password with anyone.

[162] As previously noted, the employer had the burden of proof. I find that the facts in the last two paragraphs alone provide compelling evidence that the grievor accessed his account on the four stated dates. However, before coming to a final determination, it is necessary to fully consider all the remaining evidence and assess the credibility of the grievor's account of events.

[163] The grievor steadfastly denied accessing his account on April 4, 2019, and on March 23 and 24 and April 1, 2020. He argued that his account was hacked on April 4, 2019, which was the date of the first unauthorized access and could be the reason for all the other unauthorized accesses. Specifically, he claimed that the fact that his team leader took his computer on March 29, 2019, supported his theory that his computer had been compromised in such a way that all subsequent accesses were related to that event. He claimed that on April 4, 2019, he called the IT Help Desk because he was unable to log in to his computer. He claimed that he spoke with Mr. Morris, who informed him that his computer had been hacked. He claimed that he then told his team leader, Mr. Romanelli, about it. He claimed that the close proximity of those two

events increased the likelihood that his account was compromised when his computer was taken on March 29, 2019.

[164] For the reasons that follow, I find that his story lacks credibility.

[165] Considering first the incident in which the grievor's team leader took his computer on March 29, 2019, he testified that just before then, he logged out of his computer but did not shut it down completely before going to the bathroom. When he returned, his team leader took his computer but did not close it properly, as had been the usual process when his temporary contracts ended. He implied that his team leader, with whom he had an acrimonious relationship, or someone else might have taken his computer and compromised it in such a manner that they were able to later log in to his accounts.

[166] I note that those events occurred on a Friday and that it was the last working day of his temporary contract that was set to end on March 31, 2019, a Sunday. By his admission, at the end of each of his temporary contracts, his team leader would take his computer. As such, I find that the fact that his team leader took his computer on March 29, 2019, was not unusual but rather was part of a normal end-of-contract protocol. Further, for his team leader or anyone else to log in to his account, immediately or subsequently, they would have required the grievor's passwords. Both Ms. Stockdale and Mr. Mongrain testified that passwords were required to log in to the CRA's systems. The grievor did not testify that he shared them. That evidence weighs in favour of the argument that no one later logged in to his account.

[167] The grievor alleged that on April 4, 2019, he called the IT Help Desk since he was unable to log in to his computer. He stated that he spoke with the IT agent, Mr. Morris, and that he was told that his computer had been hacked. He stated that Mr. Morris then asked him to shut down his computer so that it could be rebooted and that he then told him that his computer was fine.

[168] There is no record to corroborate that claim. Ms. Stockdale and Mr. Mongrain both testified that all calls to the IT Help Desk are logged. IT agents are required to record information about a call into Remedy. Further, Vocals automatically creates a log of all calls made to the IT Help Desk, whether answered or abandoned. Copies of those logs were entered into evidence. Based on them, the grievor did not call the IT Help Desk on April 4, 2019.

[169] At adjudication, the grievor insisted that the call to the IT Help Desk occurred on April 4, 2019, and not on April 2, 2019. However, his belief was based purely on his memory and was inconsistent with his October 27, 2020, email, in which he stated that he remembered vividly that it had occurred "around that time". His memory's accuracy was challenged further by the fact that he testified that he took no notes of the call and that his testimony occurred approximately five years after the fact.

[170] Although no record exists of a call being made on April 4, 2019, the IT records do show that the grievor contacted the IT Help Desk on April 2 and 5, 2019. Neither call was about his computer being bugged or hacked.

[171] The April 2, 2019, call resembled the grievor's description of it since it related to him not being able to log in to his computer. Mr. Morris took the call.

[172] Mr. Mongrain testified that it was not an uncommon type of call. He stated that it occurred when another user logged in to an employee's computer and forgot to log off. He stated that it could happen when an IT agent had to perform a system upgrade for a user. I note that the grievor started a new temporary contract in a different work location on April 1, 2019, and that on March 30, 2019, his then-supervisor requested that the grievor's account be modified. That provided a plausible explanation for the grievor's issue on April 2, 2019.

[173] Most compellingly, Mr. Mongrain stated that a computer being bugged or hacked is a very serious matter for the CRA and that it would have required making an escalation within his branch and conducting an investigation. In light of the seriousness of the issue, I find that it is highly improbable that Mr. Morris would have merely asked the grievor to reboot his computer to fix it, that nothing else would have been done, and that no record would have been made of it.

[174] The grievor also stated that he reported to his supervisor Mr. Romanelli that his computer had been hacked. Mr. Romanelli categorically contradicted the grievor's story. He confirmed that he was the grievor's team leader in April 2019. However, he firmly denied the grievor ever telling him that his computer had been bugged or hacked. He stated that that would be a very serious matter and that he would have recalled had it occurred. He stated that in his 20 years at the CRA, he has never heard of an employee's computer being hacked.

[175] All that evidence weighs heavily in favour of the grievor's story being false.

[176] The grievor argued that the allegations did not make sense since there was no reason for him to look at the information in his CRA account. I find that the evidence pointed to the contrary. Just as there was evidence that he had motivation to look for the refund information on October 15, 2020, all the other accesses occurred between late March and early April — when his income tax returns were due. That again provided a plausible explanation for his motivation to look at his CRA account.

[177] The grievor also argued that it was not possible that he viewed the screens identified in some of the OTIS logs since he did not use the F7 and F8 functions keys that were identified in the screen replays. Mr. Fazio testified that OTIS is very old and that one must use those function keys to navigate in it. The grievor testified that he used the F3 function key. He also admitted that he based his testimony on what he recalled but that it had been a while since he had used OTIS. When that is balanced against all the other evidence, I find that it was more likely that the grievor was in error when he claimed not to have used F7 and F8.

[178] The grievor also tried to argue that it was not possible for him to have viewed multiple screens at once since he used only one screen, despite having two at his disposal. Based on the overwhelming weight of all the other evidence, I find that explanation of little credible value.

[179] Returning to *Faryna*, a witness's story must be in harmony with the preponderance of the probabilities that a practical and informed person would readily recognize as reasonable in that place and in those conditions. The grievor's story fails to do so. I find that the evidence overwhelmingly supports the determination that he accessed his account on April 4, 2019, and March 23 and 24 and April 1, 2020, as set out in the audit log.

2. The aggravating factors

[180] In addition to the unauthorized accesses, the employer's termination letter also relied on these several aggravating factors:

- the unauthorized accesses being repeated multiple times over the 18-month span;

- the grievor's 3 attempts to conceal his misconduct and deceive the employer; and
- his failure to show remorse or an understanding of the gravity of his misconduct.

[181] I will now review each factor.

a. Repeated misconduct

[182] For the reasons explained earlier in this decision, I find that the grievor accessed his account, as indicated in the audit logs. This repeated misconduct occurred 5 separate times over a span of 18 months. He testified that over that period, he was aware that he was prohibited from accessing his account. Yet, as the evidence established, he did it anyway. It was possible that he was lulled into a false sense of security that he would not get caught since nothing happened before October 2020. However, it does not take away from the fact that each time, he was aware that he should not do it.

[183] The fact that the incidents took place over an 18-month period also mean that he continued to receive reminders in the intervening periods from the employer that that behaviour was not allowed. Five times, he decided to do it anyway.

b. Concealment and deception

[184] Mr. Jones testified that he first met with the grievor to discuss the unauthorized accesses on October 23, 2020. During that meeting, the grievor denied accessing his account on April 4, 2019, and March 23 and 24 and April 1, 2020. He admitted to accessing his account on October 15, 2020, but stated that it was in the context of training and that he had received permission from his trainer.

[185] The grievor was given a copy of the interview notes and the opportunity to make any modifications. He did not make any. But he did provide a separate email on October 27, 2020, which included some additional explanations. In them, he referred to having many IT problems during the times at issue that necessitated providing remote access to the IT Help Desk for resolution. He suggested the possibility that an IT agent might have accessed his computer. He also claimed that an IT agent told him that his account had been hacked.

[186] Ms. Stockdale testified that each explanation was investigated. Mr. Jones testified that the grievor was provided with a copy of Ms. Stockdale's investigation report and that he was invited to attend a disciplinary hearing, to discuss its findings. At that hearing, the grievor maintained that he did not access his account the first four times and that he had received permission to on October 15, 2020. He maintained that in April 2019, he was told that his computer had been hacked.

[187] The grievor testified that he received a copy of the disciplinary interview notes and that he was given the option to make changes to them. He did not make any.

[188] During the adjudication hearing, the grievor testified on his behalf. He had the opportunity to correct the record. He chose not to. As his representative stated, the grievor maintained the same story.

[189] I already addressed at length why I found that the grievor accessed his account on the five times set out in the audit logs and why his stories of the events of October 15, 2020, and of being hacked in April 2019 are not credible.

[190] With respect to his suggestion that an IT agent might have accessed his account inadvertently after remotely accessing his computer, I note that none of the accesses occurred on a date on which the grievor called the IT Help Desk. Further, Mr. Mongrain testified that IT agents do not have access to employee passwords and do not ask for SINs. Therefore, this is not a plausible explanation.

[191] Based on the totality of the evidence, I find that the employer established that three times, the grievor attempted to conceal his misconduct and to deceive it.

c. Absence of remorse

[192] It was undisputed that the grievor steadily refused to admit to any wrongdoing. As a result, there is no evidence of remorse.

[193] As a result of everything just recounted, I find that all the aggravating factors that the employer relied on were established as claimed.

[194] Since I have found that the grievor knowingly engaged in the unauthorized accesses of his account 5 times over 18 months, repeatedly attempted to conceal them after they came to light, misled the employer, and refused to acknowledge wrongdoing

or to show any remorse, it is abundantly clear that his conduct warranted disciplinary action.

B. Was the termination excessive in all the circumstances?

[195] I find that the termination was not excessive in the circumstances, for the reasons that follow.

[196] Ms. Tourigny testified that the fact that the grievor accessed his account five times over a lengthy period demonstrates that they were not spur-of-the-moment incidents. She stated that had he admitted to the unauthorized accesses when he was first confronted with them, likely, he would have received only a 30-day suspension. However, when she considered his behaviour after the accesses came to light, it changed her opinion. She stated that his absence of remorse, refusal to admit to any wrongdoing, and attempts to conceal the truth and misguide the investigation led her to conclude that the bond of trust had been irreparably damaged.

[197] The grievor argued that as an alternative argument, if I were to determine that he improperly accessed his account, I should consider as mitigating factors the fact that he viewed only his information and not that of any third party and that there was no negative effect on the employer since the events remained within the CRA. Further, the fact that he has knowledge of the alerts makes it unlikely that he would reoffend. Finally, other than one team leader, he had a good relationship with others and was not a troublesome employee.

[198] Unfortunately for the grievor, none of those mitigating factors outweighs the seriousness of the aggravating ones. Trust is at the core of an employee-employer relationship, even more so when the employee has access to highly sensitive and personal taxpayer information.

[199] The following passages from *Campbell v. Canada Revenue Agency*, 2016 PSLREB 66, summarized well the importance of the bond of trust in the context of the CRA:

> …
>
> ***49*** *I reject the submission that the grievor's long record of good service should be a mitigating factor. If anything, his long service should be seen as an aggravating factor. He had been presented with dozens of teaching aids, reminders, and joint employer-bargaining agent supports to ensure his understanding of and compliance with the code of conduct. A long-standing employee*

> *should have greater workplace awareness and thus be more worthy of the employer's trust.*
>
> ***50*** *In the end, I did not hear any remorse from the grievor that would reflect his appreciation of the potential harm to his employer that was caused by his misconduct. He readily acknowledged that he knew that what he was doing was a breach of his code of conduct, yet he chose to repeat his misconduct many times. He testified that he wished that he had not committed the acts of misconduct, but I took that comment to mean that he regrets having lost his severance, rather than being regretful for what he has done to his employer. As such, I must reject the grievance.*
>
> ***51*** *To do otherwise and allow the reinstatement of this grievor, and other such grievors, would necessarily elevate the risk of further misconduct being committed by an employee who fully understands that what he is doing is wrong but for his own reasons chooses to regularly commit acts of misconduct against his employer. The grievor showed no understanding of the potential harm to the Canadian tax system that choosing to disregard the employer's code of conduct posed.*
>
> ***52*** *This is not a case in which progressive discipline would warrant lesser discipline, to encourage the employee's rehabilitation. For the reasons noted earlier, the bond of trust in the employer-employee relationship has been caused irreparable harm by the grievor's decision to repeatedly disregard the employer's code of conduct.*
>
> …

[200] Although the facts in *Campbell* were not the same as in this case, I believe that the same conclusions should be drawn. The grievor was a long-standing employee and had been presented several times with reminders of the Code and Directive. Therefore, he should have known better. Unlike in *Campbell*, the grievor in this case refused to acknowledge any wrongdoing or accept responsibility for his actions. In fact, it is telling that he was unable to refer me to a single case in which an employee refused to admit to wrongdoing but nonetheless was reinstated. He referred me to the following five decisions where lesser disciplinary penalties were substituted or considered.

[201] In *Nova Scotia (Public Service Commission) v. NSGEU (Hillier)* (2013), 238 L.A.C. (4th) 62, the grievor in that case was discharged for improperly accessing customer-service information for purposes not related to business. The grievor did not dispute that there was just and sufficient cause to impose discipline but argued that the discharge was excessive in the circumstances. Although the grievor had lacked candour when she was initially confronted about the breach, the discussion occurred

in a casual setting, and she confessed immediately within the following 24 hours. She apologized, supplied the employer with documentation to explain her actions, and cooperated during the investigation. Given those facts, the arbitrator found that the employment relationship had not been so irreparably damaged that it could not be restored. In that context, the arbitrator found that the discharge had been excessive.

[202] In *Eastern Regional Integrated Health Authority v. NAPE (O. (L.))* (2015), 259 L.A.C. (4th) 188, the grievor in that case worked in a hospital and had been suspended for improperly accessing patient records. She had accessed her and her father's records as a teaching tool for co-workers and a physician. She admitted to her wrongdoing.

[203] Similarly, in *Newfoundland and Labrador Nurses' Union v. Eastern Regional Integrated Health Authority*, 2014 CanLII 83846 (NL LA), a grievor was terminated for accessing unauthorized information. Once again, the grievor admitted her wrongdoing.

[204] In *Mercer v. Deputy Head (Department of Human Resources and Skills Development)*, 2016 PSLREB 11, a grievor was terminated for giving preferential treatment to family members while providing services. Although the grievor fully cooperated in the investigation, he denied wrongdoing on the basis that he had not been aware that it was wrong. The former Board declined to reduce the disciplinary penalty and noted that the grievor had demonstrated no remorse for his actions and had repeatedly tried to deflect responsibility for them by blaming the employer for his ignorance or alluding to others doing the same thing.

[205] In *Peel (Regional Municipality) v. CUPE, Local 966 (Trotman)* (2016), 273 L.A.C. (4th) 117, the grievor was a case worker and was terminated after accessing her daughter's file. The issue in that case was whether her action had caused her daughter to receive a payment. Although the grievor was not completely truthful when first confronted with the situation, she later admitted to viewing the information. But she denied that she triggered the payment. The arbitrator agreed, reinstated the grievor, and substituted a five-day suspension as the penalty.

[206] I draw from all that case law the importance of admitting to a wrongdoing, accepting responsibility, showing remorse, and cooperating in an investigation. As trust is at the root of the employer-employee relationship, I can hardly see how the

grievor could be reinstated in the absence of any such evidence. The bond of trust cannot be repaired without it.

[207] The CRA is entrusted with the most personal and sensitive of taxpayer information. It must act when breaches occur, as the public's confidence depends on it. While it is true that the grievor viewed only his account and arguably derived little benefit from it, it did not take away from the fact that doing so violated the Code and the Directive and that he repeatedly did it anyway.

[208] When that is compounded with the damage caused by his refusal to admit to the wrongdoing, the attempts to conceal it, the fabrication of stories to avoid responsibility, and the absence of any remorse, I conclude that the termination was warranted.

[209] For all of the above reasons, the Board makes the following order:

(The Order appears on the next page)

IV. Order

[210] The grievance is denied.

June 10, 2025.

Audrey Lizotte,
a panel of the Federal Public Sector
Labour Relations and Employment Board