Legislative Assembly of Alberta

The 29th Legislature
Second Session

Standing Committee
on
Public Accounts

Advanced Education
NorQuest College

Tuesday, December 6, 2016
8:32 a.m.

Transcript No. 29-2-11

Legislative Assembly of Alberta
The 29th Legislature
Second Session

Standing Committee on Public Accounts

Fildebrandt, Derek Gerhard, Strathmore-Brooks (W), Chair
Anderson, Shaye, Leduc-Beaumont (ND), Deputy Chair

Barnes, Drew, Cypress-Medicine Hat (W)
Cyr, Scott J., Bonnyville-Cold Lake (W)
Dach, Lorne, Edmonton-McClung (ND)
Fraser, Rick, Calgary-South East (PC)
Goehring, Nicole, Edmonton-Castle Downs (ND)
Gotfried, Richard, Calgary-Fish Creek (PC)
Hunter, Grant R., Cardston-Taber-Warner (W)
Luff, Robyn, Calgary-East (ND)
Malkinson, Brian, Calgary-Currie (ND)
Miller, Barb, Red Deer-South (ND)
Renaud, Marie F., St. Albert (ND)
Turner, Dr. A. Robert, Edmonton-Whitemud (ND)
Westhead, Cameron, Banff-Cochrane (ND)

Also in Attendance

Taylor, Wes, Battle River-Wainwright (W)

Office of the Auditor General Participants

Merwan Saher	Auditor General
Robert Driesen	Assistant Auditor General
Diana Potapovich	Principal

Support Staff

Robert H. Reynolds, QC	Clerk
Shannon Dean	Law Clerk and Director of House Services
Trafton Koenig	Parliamentary Counsel
Stephanie LeBlanc	Parliamentary Counsel
Philip Massolin	Manager of Research and Committee Services
Sarah Amato	Research Officer
Nancy Robert	Research Officer
Corinne Dacyshyn	Committee Clerk
Jody Rempel	Committee Clerk
Aaron Roth	Committee Clerk
Karen Sawchuk	Committee Clerk
Rhonda Sorensen	Manager of Corporate Communications and Broadcast Services
Jeanette Dotimas	Communications Consultant
Tracey Sales	Communications Consultant
Janet Schwegel	Managing Editor of *Alberta Hansard*

Transcript produced by *Alberta Hansard*

Standing Committee on Public Accounts

Participants

Ministry of Advanced Education
- Mr. Peter Leclaire, Assistant Deputy Minister, Advanced Learning and Community Partnerships
- Mr. Rod Skura, Deputy Minister

NorQuest College
- Jodi Abbott, President and Chief Executive Officer
- Joan Hertz, Vice-president, External Affairs, and Corporate Counsel
- Jill Matthew, Vice-president, College Services, and Chief Financial Officer
- Alan Skoreyko, Board Chair

8:32 a.m. Tuesday, December 6, 2016

[Mr. Fildebrandt in the chair]

The Chair: Good morning, everyone. I'll call this meeting of the Public Accounts Committee to order and welcome everyone in attendance. I'm Derek Fildebrandt, chairman of the committee and the MLA for Strathmore-Brooks.

I'll ask that members, staff, and guests joining the committee at the table introduce themselves for the record, beginning to my right.

Mr. S. Anderson: Morning. I'm Shaye Anderson, deputy chair, MLA for Leduc-Beaumont.

Mr. Malkinson: Hello. Good morning. Brian Malkinson, MLA for Calgary-Currie.

Ms Miller: Good morning. Barb Miller, MLA, Red Deer-South.

Mr. Westhead: Morning. Cameron Westhead, MLA for Banff-Cochrane.

Ms Renaud: Good morning. Marie Renaud, St. Albert.

Ms Luff: Good morning. Robyn Luff, MLA for Calgary-East.

Mr. Dach: Good morning. Lorne Dach, MLA, Edmonton-McClung.

Dr. Turner: Bob Turner, Edmonton-Whitemud.

Mr. Gotfried: Richard Gotfried, MLA, Calgary-Fish Creek.

Mrs. Matthew: Jill Matthew, vice-president of college services and chief financial officer.

Mrs. Hertz: Joan Hertz, vice-president, external, and corporate counsel at NorQuest College.

Dr. Abbott: Good morning, everyone. Jodi Abbott, president and CEO of NorQuest College.

Mr. Skoreyko: Alan Skoreyko. I'm the board chair at NorQuest College.

Mr. Skura: Rod Skura. I'm the Deputy Minister of Advanced Education.

Mr. Leclaire: Peter Leclaire, assistant deputy minister, advanced learning and community partnerships within Advanced Education.

Ms Potapovich: Diana Potapovich, office of the Auditor General, and I'm an engagement leader for the audit of NorQuest College.

Mr. Driesen: Rob Driesen, Assistant Auditor General.

Mr. Saher: Merwan Saher, Auditor General.

Mr. Taylor: Wes Taylor, MLA, Battle River-Wainwright.

Mr. Cyr: Scott Cyr, MLA, Bonnyville-Cold Lake.

Mr. Barnes: Good morning. Drew Barnes, MLA, Cypress-Medicine Hat.

Mr. Hunter: Good morning. Grant Hunter, Cardston-Taber-Warner.

Ms Robert: Good morning. Nancy Robert, research officer.

Dr. Massolin: Good morning. Philip Massolin, manager of research and committee services.

Mrs. Sawchuk: Karen Sawchuk, committee clerk.

The Chair: Thank you.

As you'll notice, we have Wes Taylor joining us at the table today.

Nicole Goehring, I believe, is on the line. If you want to introduce yourself.

Ms Goehring: Good morning. Nicole Goehring, MLA, Edmonton-Castle Downs.

The Chair: We have a few housekeeping items before we turn to the business at hand. The microphone consoles are operated by *Hansard*, so there's no need to touch them. Audio of committee proceedings is streamed live on the Internet and recorded by *Hansard.* Audio access and meeting transcripts are obtained via the Legislative Assembly website. Please turn your phones to silent.

Are there any changes or additions to the agenda as presented? Seeing none, would a member move that the agenda for the December 6, 2016, meeting of the Standing Committee on Public Accounts be approved as distributed? Moved by Mr. Hunter. Any discussion? All in favour? Opposed? Carried.

Do members have any amendments to the November 29 minutes as distributed? Seeing none, would a member move that the minutes of the November 29, 2016, meeting of the Standing Committee on Public Accounts be approved as distributed? Moved by Ms Miller. Discussion? All in favour? Opposed? On the phone? Carried.

All right. I'd like to welcome our guests from NorQuest College and the Ministry of Advanced Education, here today to speak to the financial systems in place to prevent potential fraudulent activity and privacy breaches. The Auditor General initially addressed this issue in his March 2012 and February 2013 reports, and the committee met with NorQuest College in April 2013.

Members should have the committee research document prepared by research services and the Auditor General's briefing document as well as the updated status of Auditor General recommendations documents completed and submitted by NorQuest College and by the Ministry of Advanced Education.

I'll now invite officials from NorQuest College to provide opening remarks, not exceeding 10 minutes.

Dr. Abbott: Thank you very much, Chair. We're pleased to be here today to respond to any questions you have. I don't want to assume that you know a lot about me or about NorQuest College and the impact that we have in our community. I was officially sworn in as president and CEO of NorQuest College over six years ago. When I looked at the NorQuest College of the future, I imagined an amazing transformation: programs that would allow students to achieve, excel, and fulfill their dreams; a college that transforms the way people access education; a college that transforms regional communities, ensuring these communities remain viable to the people who live, work, and learn in them. Today we are well on our way to creating that college.

Through changes in government, budgetary fluctuation, shifts in the economy, and more, my vision for NorQuest College has remained intact, if not firmer than before. Students enter NorQuest College ready to step forward with their lives and leave with the skills and confidence to succeed. NorQuest does more than change the lives of its students; we're changing our communities.

When you walk into a hospital or a continuing care centre, you're likely to see NorQuest grads busy as unit clerks, licensed practical nurses, or pharmacy techs. Local businesses are running with the

help of our accounting tech, admin professionals, and business admin grads. Our communities rely on our social work, community support workers, day home providers, and early learning and child care graduates.

We prepare students to be successful at any level. Whether it's literacy skills, ESL, or academic upgrading, NorQuest College is honoured to support our students in achieving their dreams, and we are proud that 57 per cent of NorQuest students are born outside of Canada, representing 134 countries, with over 70 languages spoken.

NorQuest College was the target of an alleged fraud and misconduct relating to confidential information and financial assets between 2008 and 2012. Once we discovered that NorQuest College was a victim of the misconduct in early 2013, we informed the board of governors and took swift and decisive steps with the best interests of students, employees, and the public in mind. Today I'm pleased to report that we have now successfully concluded the legal settlement of the alleged fraud and privacy breach and secured the information, and due to ongoing work over the past four years, we are confident we have strong controls in place to protect our people and our assets.

Through the course of this matter the courts awarded us legal remedies rarely given which enabled the college to recover all confidential information and college assets related to the alleged fraud from various avenues. This is reported in the college's 2015-16 financial statement, which reports $1.622 million in other revenue with a note explaining that the college recovered funds related to an alleged fraud that occurred between 2008 to 2012. The $1.622 million includes not only the total estimated losses but the costs as well.

8:40

I must emphasize that our primary concern throughout the matter has been to protect the people targeted and the college as a whole. From the beginning we made a commitment to be diligent, work alongside investigators, and follow due process. As a leader in postsecondary education and in the spirit of openness and transparency we will share our learnings with other postsecondary institutions to help them guard against this type of fraudulent activity and protect their employees and students.

We became aware of the alleged misconduct in early 2013 when a former employee, previously terminated, Clarence Orleski, allegedly sent inappropriate electronic messages to various people. We worked quickly and decisively to identify and stop the alleged harassment. We obtained a rare court order, known as an Anton Piller order, which allowed, without warning, an extensive search of Orleski's home on March 2, 2013. This led to the recovery and securing of NorQuest College property and information in the possession of Orleski, including electronic devices, by the bailiff.

To protect those whose information may have been compromised, only forensic investigators and two NorQuest officials were permitted to view the materials and only for the matters related to the specific legal action. As stipulated in the court order, the bailiff retained all of the seized property and information recovered. The legal remedies we obtained were unique. The college was able to quickly secure all of the electronic data and also restrain the actions of Orleski by court order. For example, under the terms of the March 2 court order Orleski is prohibited and restrained from accessing or making use of any confidential information obtained or created in the course of his employment with NorQuest, and violating this court order in any way would be considered contempt of court, with serious repercussions which could include imprisonment.

As governed by the legal parameters and the lengthy and complex review of the seized devices, this took place over the summer and fall of 2013. Through the course of the review further alleged misconduct was discovered. NorQuest uncovered an intricate set of allegedly fraudulent transactions dating back to 2008 and totalling approximately $1.2 million, which led to further investigation and legal actions. Through a series of contracts and payments related to the provision of services and equipment to NorQuest, Orleski and a number of external individuals and companies allegedly colluded to defraud the college.

The NorQuest finance team and the CFO discovered a string of questionable transactions, and NorQuest retained EY to perform forensic accounting investigations and confirm the alleged fraud. With this information, we further obtained the extraordinary legal remedies of a Mareva injunction and Norwich orders in order to freeze the assets and require third parties to produce relevant documents and information related to the alleged fraud.

As I stated earlier, we were able to maximize our efforts to recover the funds lost and costs related to the recovery through various avenues. From the start, NorQuest worked with the two employees directly targeted by the privacy breach to inform them, protect their privacy, and resolve the issue as quickly as possible.

As for broad disclosure, legal counsel advised us from the beginning of this matter that due to a pending criminal investigation by the Edmonton Police Service, ongoing litigation, restrictions around the use of seized records, and emerging evidence of an alleged fraud perpetrated against the college, there was a risk that broad disclosure of the privacy breach would hinder both the criminal and civil investigations.

It's important to note that legal counsel deemed the risk of harm to the majority of college employees to be low as all records had been secured. Nevertheless, when NorQuest received confirmation from EPS that providing employees with more information would not impede their current investigation, we informed all employees and stakeholders of the situation. This occurred in early September 2016. I'd like to emphasize that if the college had any evidence or suspicion that other employees or students were at risk during this process, we would have immediately followed up with them directly.

During the course of these matters NorQuest worked diligently to make sure that we took proper courses of action. This included advising the EPS, the office of the Auditor General, the Ministry of Advanced Education, and the office of the Information and Privacy Commissioner of Alberta although FOIP legislation does not require it. In addition, we acted under legal advice and court direction.

We are committed to being as open and clear as possible. That is why over the past few weeks we have completed a further search of the records, which have been secured since March 2, 2013, to determine if Orleski had accessed other NorQuest information. The results of the search indicate that the vast majority of records were work-related e-mails or meeting notices. The search did not disclose any personal information that would be considered highly sensitive in nature such as social insurance numbers, banking or medical information. A very small number of records contained information related to salary, performance, and similar matters.

We are in the process of contacting people by letter outlining the details of the information found. We have also provided a detailed update to all of our employees. Again, there is no evidence to suggest that this information was used in any way by Orleski or that it entered the public domain.

Going forward, I am confident our internal controls and systems are secure. This has been confirmed by extensive reviews over the past four years. This has also been verified by the office of the Auditor General in their last three reports and in testing by

independent third-party experts. Details about NorQuest College's strengthened controls can be found in our annual reports.

Finally, I'd like to point out that in many cases involving internal fraud and misconduct, particularly where there is alleged collusion with outside parties, not only is it difficult to detect, but recoveries of assets are rare. I'm pleased to report that we were one of few organizations to be able to successfully recover our assets. In fact, NorQuest College is among only 12 per cent of organizations to recover assets from alleged fraud, as substantiated by the 2016 Report to the Nations on Occupational Fraud and Abuse.

The Chair: Thank you very much for your opening statement.

Dr. Abbott: Chair, could I just ask our legal counsel to make one statement? It's around the parameters of our conversation, around the legal parameters. It'll take one second.

The Chair: Very well.

Dr. Abbott: Thank you.

Mrs. Hertz: As the lawyer who's going to talk for one second, I just wanted to talk about the use of the word "alleged" today. You're going to hear us say "alleged" in front of conduct describing the conduct of individuals or the conduct of companies today, and the reason for that is that the allegations that we're talking about were not proven in court. They were resolved by legal settlements. So in order to preserve the recoveries that NorQuest College has made and also just to be careful that we are not improperly alleging conduct that was not proven in court, you'll hear us say "allegedly," and all of us should be careful to use that language. But if we don't, I just wanted to ask that it be inferred that we meant to say "allegedly" before the conduct described.

The Chair: Very well. Thank you very much for that.

We'll now give the floor to the Ministry of Advanced Education for their comments, to not exceed five minutes.

Mr. Skura: We have no opening comments.

The Chair: Thank you very much. More time for questions. That's what I like.

I'll now ask the Auditor General for his comments.

Mr. Saher: Thank you, Chair. Every organization is inherently subject to the risk of fraud. Well-designed and effective internal controls and processes can substantially reduce the risk of fraud but cannot eliminate it. In particular, the strongest of internal control environments won't stop fraud perpetrated through collusion.

Audits are not designed to detect fraud. An audit can highlight how significant weaknesses in internal controls and processes make the risk of fraud greater. On page 83 of our February 2013 report we warned NorQuest College that its 10 outstanding internal control recommendations exposed the college to fraud and error going undetected. Unknown at the time was that during fiscal 2008 to 2012 transactions had occurred which were later identified by management in fiscal 2014 as an alleged fraud.

Management made significant improvements to internal controls and processes in fiscal 2013 and implemented the majority of their outstanding recommendations from the Auditor General's office. In fiscal 2013 and since, we have been able to conclude that the college has adequate internal controls and processes to reasonably mitigate the risk of fraud and error.

We have read the college's 2016 annual report, which includes disclosures made related to the alleged fraud, information privacy breach, and recovery of funds. We have concluded that the disclosures made in the annual report, which include the college's fiscal 2016 financial statements, are factually correct and consistent with the understanding we obtained in completing our audit.

Thank you.

8:50

The Chair: Thank you very much.

We'll now open the floor to questions from members of the committee, beginning with eight minutes for members of the Official Opposition. Mr. Taylor.

Mr. Taylor: Thank you, Mr. Chair, and thank you to everybody that has shown up today. I have several questions here with regard to, I guess, the massive privacy breach. That's why we're here. When we're looking here from April 24, when the college had seized its former IT manager's personal computer, to March 2013, you had enough information to convince a judge to award you that rare court order, the Anton Piller. Why didn't you at that point in time tell the staff, your faculty, what was happening? This is a massive privacy breach, and you knew something was wrong. That's how you got the Anton Piller. I need an explanation as to why that was not brought up.

Dr. Abbott: I'm happy to answer your question, hon. member. What I would do is take you back to 2012, when we were managing the performance of this particular individual. What happened is that in early January a series of e-mails went out that were particularly targeting two individuals. Through the assessment of those e-mails, the information that we had available to us, what we were able to do was go to the courts and say: "We're very concerned about this. We're concerned because these individuals have families." Their families were being impacted by this. Through the Anton Piller order we were able to secure all of the information. The Anton Piller order allows you to go on a surprise basis into someone's home. So we were able to gather all of that information.

At that point in time all information was secure. That information was secure. The two individuals that were directly targeted by the perpetrator: we had them fully informed. We had absolutely talked to the two individuals. In fact, they became part of the civil litigation.

You have to remember that we were focused on that alleged harassment of those two individuals as we gathered that information. As you can imagine, you go into someone's home. You gather their personal computer, which we were able to secure, as well as some other devices. You actually have to take that information, put it into a searchable file structure, so we had hired a company to help us to do that. We were specifically looking at the alleged fraud. In the process of that – we were doing the reviews – it took us all the way to the summer before we discovered the alleged fraud.

When you go back to broad disclosure, one of the things we know is that, one, we had done disclosure to the two individuals impacted. Our legal counsel had advised that it was very low risk to other employees in the college. If we would have disclosed, we likely would not have been able to get the Mareva injunction or the Norwich orders because the Norwich order and the Mareva injunction allow us to freeze assets as well as gather bank account information. In the summer-fall is when we noticed potentially fraudulent activities.

So we had secured the information. We followed the steps outlined in the OIPC guidelines. The first thing you do is secure information. We had been given advice from legal counsel that the risk of harm to others was extremely low, and we were dealing with those with the highest risk.

Mr. Taylor: Okay. Thank you.

So why did it take over a month to start to search the computer?

Dr. Abbott: What happened is that, first of all, we had multiple devices. It wasn't just one computer. We had the home computer plus some devices. You actually have to create a file structure. We had to hire a company. I think that at that time the company we used was called Urgentis. They came in. They actually take all of the information from the bailiff in a supervised fashion. They have to create file structures, and those file structures take time. Then we had to search them. There was a high volume of records. It took time to create the structure and then go through it. So if you're asking if we knew about this when we came to Public Accounts in 2013, we did not because we were in a process to pull together the information to be able to search it.

Mr. Taylor: You knew about the information – that's how you got the Anton Piller awarded – so you had a duty to tell, I think, the Public Accounts Committee at that point in time that there was a breach. That was part of the question that was going on. Why did you not tell the committee, the PAC, at that point in time that there was a massive security breach? I mean, I understand that you could maybe not go over the details because you were still trying to find out those details, but you knew about a variety of the details because you had, like you say, enough information to be able to get that awarded so you could have that search and seizure of the computer of Clarence Orleski.

Dr. Abbott: I think there are a couple of things. First of all, we didn't know how broad the breach was. We went into the courts. We were suspecting that this particular individual was the individual that was targeting two individuals. So we were really managing around those two individuals. We had secured the data. When we came forward to Public Accounts, the infrastructure was still being built, so we, again, were in process.

We also went forward to Public Accounts to respond to previous years' annual reports, so that was the focus of Public Accounts at that time. I would say that at that time management at NorQuest College was managing the issue, and we didn't know all of what was ahead of us. As you can tell from the timeline that I went through in my opening remarks, all of the review took a lot of time because it was very, very complex.

Mr. Taylor: It just seems to me that you obfuscated that responsibility by not telling the Public Accounts Committee.

My question, I guess. The AG identified that NorQuest College needs to improve internal controls in order to reduce potential risk of fraud and inaccurate financial information. There were eight recommendations made, and it said, "We believe the majority of the recommendations are making satisfactory progress." Do you feel the statement might be slightly inaccurate given that at the time you had just confiscated Orleski's computer?

Dr. Abbott: No. What I would say is that when you identify that you have an internal controls challenge, which the office of the Auditor General did – I joined the college in 2010. We have to remember that the alleged fraud began in 2008. So the first thing is that we started to improve our internal controls. We got very clear feedback from the office of the Auditor General, and in that feedback what we did was that we brought in a company to assist us. So PricewaterhouseCoopers developed something called an ICOFR project, which is the internal controls over financial reporting.

Through that process we developed new policies and procedures. We tested the policies and procedures. We had to educate our staff on internal controls because it's really important that they have a strong understanding. When you are changing internal controls in an organization, it definitely is a culture shift, so you have to educate people. The average person in an organization wouldn't even understand the words "internal controls," so what you have to do is educate people so that you actually get a change in behaviour.

The Chair: Thank you.

Eight minutes for members of the government.

Ms Renaud: Thank you. Dr. Abbott, we heard that NorQuest was in contact with the Information and Privacy Commissioner during the alleged fraud and privacy breach. In fact, I think you just said that you followed the guidelines as laid out by the office. Why didn't NorQuest report the breach to the Privacy Commissioner earlier?

Dr. Abbott: What happened: one of the guidelines is that you secure the data, so we had secured the data. Our legal counsel advised that the majority of people would be at low risk because the data had been secured. The two individuals that were directly targeted: we were working directly with them. So in terms of the guidelines, it's contacting the individuals who have been directly targeted or impacted and working through that with them. They were well aware of the information as well as the process we were going through. In fact, they became part of the civil litigation process along with us. We had secured the data. Through the OIPC legislation it's not required by law that we do contact them. We made a decision to contact them because we were proceeding further in terms of the alleged fraud, so we made calls to them to let them know: here's where we're at in the process; the data has been secured.

What we did not do is ask for an investigation. The reason we didn't do that is that all of the data had been secured and we had been working very directly with those specifically targeted.

9:00

Ms Renaud: Okay. Can you just maybe back up a little bit? In more detail, what work did NorQuest do with the Privacy Commissioner to address the actual breach?

Dr. Abbott: In September 2016 at the broadest level NorQuest College contacted the EPS to talk to them about whether we can talk more broadly about this because we were being very careful not to impede either the civil litigation or the criminal investigation that was going on, and their counsel indicated that we could now disclose more broadly to our employees. We did that. We had multiple communications with our employees. During this time we were speaking directly with the OIPC to ensure that they were aware of our communications. We also encouraged and the OIPC encouraged that if anyone was concerned about this, they could contact the OIPC and identify a complaint.

I will tell you that in the process there were four individuals that came forward. Two internally came forward because when we sent out the communication, we said that we're willing to meet with anyone who's concerned. So two internal employees came forward. We also met with our AUPE executive and our faculty association executive and informed them where things were at. We had three former employees that made a complaint to the office of the Information and Privacy Commissioner. We have now concluded the review of those specific files. In those cases, as I said in the opening, there was nothing sensitive of a confidential nature. There were no social insurance numbers, no banking information, no medical information. We have been in contact with all of those individuals.

Ms Renaud: I am glad to hear that NorQuest has implemented finally, some of them quite old, the recommendations from the Auditor General and that you now have adequate systems in place to mitigate the risk of fraud and privacy breaches. I'm wondering specifically about the internal controls and processes that have been changed. Which are new, and which are changed going forward?

Dr. Abbott: I'm happy to answer. I'll answer, and then I may pass over to Jill, our CFO, in case I miss anything. Through the ICOFR project we identified two kind of primary categories of control, one on our IT systems and the second on our financial systems.

If I start with the financial system, some of the things we've put in place, first of all, we have updated all of our financial policies and procedures. Our procurement process and procedure have changed. In the past, in the far past an individual could set up a vendor without having a second person approve it. Now all procurement set-up of any vendor goes through our procurement department, and it has to be signed off by a senior person in the organization. We put that kind of control in place. We've also put segregation of duties in place, which is very important. An example of that is an employee who may have an expense for something, maybe just a parking expense. They can't approve their own expense. That's an example of segregation of duties. Those are two examples on the finance side.

On the IT side we do the monitoring of who is accessing what. Every employee has certain access to particular files or computer systems, and what we have now is monthly monitoring that happens. We can look at logs of who's been looking at what kind of documents to ensure that they're only looking at what they should be looking at. Those are a couple of examples.

Ms Renaud: Okay. I just have a quick question. Just to skip back a little bit, are you satisfied or is management satisfied that there is, I guess, very little difference between the information that was reported regarding the privacy breach and – I don't mean censored, but was it censored in a sense because of the legal agreement that you arrived at, the settlement?

Dr. Abbott: Joan, do you want to take that?

Mrs. Hertz: We have been able to communicate fully with our employees about what happened in the course of the alleged privacy breach. No, there is nothing that held us back from sharing anything that's in the public interest.

Ms Renaud: Okay. As you've said, this was a very significant alleged privacy breach, which affected quite a few people. I think that you mentioned that you sent a letter out in September of 2016? Is that correct?

Dr. Abbott: We sent the letter out in the last couple of weeks. It was as of September 2016 that we went in and had a couple of experts go in and look at all of the data to confirm. We did very specific searches by putting in key words like social insurance number, employee name, employee address, and medical information. That allowed us to narrow down if there was any risk of harm.

Ms Renaud: Okay. What work was done before that to communicate with those who were possibly at risk of being impacted by the breach?

Dr. Abbott: In September 2016, when the story became public, we contacted the EPS to ensure that we could speak more broadly. We communicated very broadly with our employees by putting a statement both on our internal intranet as well as the external website. It has been well communicated to all employees. We offered to those employees: would you like to come and talk to us about it? We had only two people come forward.

Ms Renaud: Thank you.

The Chair: Thank you.

Five minutes for members of the third party.

Mr. Gotfried: Thank you, Mr. Chair, and thank you to our visitors today. I've got a few questions here, and it kind of relates to the full impact of this alleged fraud and other issues here. In looking up some background articles on this, there was some mention of some payments to Cobalt Business Systems of over $2.6 million and Alcon of $717,000, which total $3.317 million or thereabouts. There is also information about termination payments made to the alleged perpetrator. There are comments about inappropriate expenses incurred by the perpetrator. There may be some other things that we're unaware of. This means that the total cost, I would say, to the public purse is somewhere in excess of $3.3 million.

We've been informed today by the Auditor General that there is a likelihood that there was a settlement in the neighbourhood of $1.6 million, which means that there is about a $1.6 million delta in here of the cost of this entire episode to the college. I think that the public should be privy to this.

I guess the other question is: for that large a dollar amount, that big a delta between the possible settlement, which is not public knowledge, and the full extent of this breach – it seems to me to be a large amount here – has the college addressed this in a way which balances the real cost to the public of the total amount here versus the decision to settle? I guess my question is that I'd like to understand the decision process in not pursuing full legal recourse versus a settlement.

9:10

Dr. Abbott: Okay. A very good question. First of all, I would say that we did pursue full legal recourse. I'll just walk through a little bit on the figures that you have provided, and I may ask Jill to step in. First of all, there was purchase of goods and services from a couple of companies. You mentioned Cobalt. There was Alcon and Cobalt. NorQuest College did receive the goods and services, but there was an upcharge on that amount, so the delta that you're maybe referencing relates to the overall cost of those goods and services that we paid, what we paid for at the time, but there is a delta in that because there was this upcharge that then moved into kickbacks to various individuals. I think that explains part of it.

We went through and our CFO and finance team went through and did benchmarking about what the typical cost is that you would pay for a particular good or service and identified what that difference was. When we did the overall total – we did the work, and then we had EY confirm the work – it was around $1.2 million. That was what the real delta was. I think that kind of gives that broad picture. Then we were able to recover $1.622 million. Just as a reminder, that included the losses that we had plus the costs in recovering the losses we had through the litigation.

Mr. Gotfried: Okay. I understand that that's some justifiable expense. I find it a little hard to believe that these companies really provided anything of necessary value to the college. There may be an opportunity to attach a dollar amount to things that were procured, but I maybe question – yes, I know you have to value these things and say, "Well, if we were to want to purchase these things," but I have some concerns with that.

The other thing here, of course, is that there has been mention of terminations and inappropriate expenses, so I do question that. You know, certainly those numbers should be, I think, disclosed to Public Accounts and to the Auditor General so that we do have a clearer picture. I think everybody wants transparency in this. Broadly speaking, I suspect that this has been a very hard lesson learned by everyone and perhaps is something that the entire postsecondary field can learn from, the fact that that's the case.

I've got one other quick question. [A timer sounded] I guess I don't.

The Chair: Your question in a few minutes.

Eight minutes for members of the Official Opposition.

Mr. Taylor: Thank you, Mr. Chair. I was kind of wondering. You were just talking about the companies that were involved with the kickbacks. Have these companies and these individuals been censured from the paying of these kickbacks, their business dealings?

Dr. Abbott: What I can say is that when we became aware of the alleged fraudulent activity, we contacted the EPS a second time. We had contacted them the first time specifically around the alleged harassment. Then we contacted them around the alleged fraud. It is our understanding that there is an investigation ongoing, so we need to let that process happen. You know, this isn't over yet because the criminal investigation is going on, and NorQuest College will work collaboratively with the EPS because we would like to see the alleged perpetrators brought to justice.

Mr. Taylor: Okay. Thank you.

Did Orleski pay back that money, or did some other individual pay back that money or some other entity?

Dr. Abbott: What I can tell you is that through the settlement – the settlement came from various sources. I know that's a broad answer, but the settlement did come from various avenues.

Mr. Taylor: Can you give me the breakdown?

Dr. Abbott: I'll just pass it to Joan.

Mrs. Hertz: If I can just comment. If we were to get into the specific breakdown of the settlements, we would risk the recovery of the amounts from the settlements because we did enter into agreements with the people who have . . .

Mr. Taylor: Yeah. So did Mr. Orleski pay any of the monies?

Mrs. Hertz: Again, if I get into the specifics of the settlement, I would be breaching the confidentiality terms.

Mr. Taylor: Okay. At a later date would you be able to disclose that?

Mrs. Hertz: No, because . . .

Mr. Taylor: Okay. Thank you.

You know, it seems preposterous that Orleski – he's an IT manager, and you're suggesting that you have all the data collected from him. Being an IT manager and the person that was able to do this for years, being able to take the data, and being able to take monies and not share it somewhere else or put it somewhere else, it seems preposterous, perhaps ludicrous to even suggest that you've collected all that data. How can you ensure to Albertans that you have all that information?

Dr. Abbott: What I would say is that, first of all, through the Anton Piller order you go in and sweep someone's home, and it's a very, very aggressive process. It's done on a surprise basis. We gathered all devices, and it included a search of a home, a garage, everything. Everything was brought together. Through that process there was a court order in place that identified that Orleski could risk imprisonment if he shared the information, if he had copied it, if he had shared it. We had everything, though. Really, everything had been secured.

I think we also have to remember that it's been almost three and a half years since this happened, and we have not seen any repercussions. If you think about the fact that we had very few staff – we have over 700 employees in the organization. Very few came forward concerned. We have had no evidence that any other information had been shared other than the two individuals that were specifically targeted.

Mr. Taylor: So could this not have been shared, I mean, just placed into the cloud, as it was? You know, people do put information into the cloud. Are you able to guarantee that you have all the information?

Dr. Abbott: What I would say, again, is that through the Anton Piller order we were able to gather everything. We had IT experts go through the data and ensure that the data was secure.

Mr. Taylor: Are you able to guarantee that you have all the data, then?

Mrs. Hertz: Maybe I can add a quick comment. I don't think there is any way to guarantee; however, the court order does bind Mr. Orleski. Through the process of the search he was required to confirm that he had not copied and that the material was not being stored elsewhere to the IT expert along with the bailiff and the supervising lawyer for the Anton Piller search. As well, there are restrictions in that court order on Mr. Orleski personally, that he not disseminate in any way, use any information that he may have gotten. If we did not for some reason recover everything and it was stored elsewhere, he is bound by court order not to use it. If he does, that could be seen as contempt of court, and he could suffer a penalty as serious as imprisonment.

Mr. Taylor: Understood.

Really, why wasn't this all brought to PAC? That's the most important question. That's why we're here today. Why wasn't this brought up to PAC back in 2013? If this was disclosed at PAC in 2013, there would not be this meeting that we're having today.

Dr. Abbott: Hon. member, as I identified earlier, we were in a process. We didn't know what we had. We were going through – all of the files were being put together, and we hadn't started to search all of that information. What we knew was about two individuals . . .

Mr. Taylor: But you knew you had a security breach.

Dr. Abbott: We had a security breach specifically about two people, and those were the two people that were targeted, so our area of focus was really looking at: how do we protect those two employees? Those two employees have families that were being impacted through this process, and we took that very seriously. In fact, those two employees participated in the litigation. It was not until the summer/fall that we had actually been able to go in and look at information.

Mr. Taylor: Okay. I have a separate kind of question for you with regard to that.

Or did you have a question that you wanted to ask?

9:20

Mr. Cyr: Yes. I guess my concern here is that you've been making pretty firm comments that you have all the information. I think you've demonstrated that you can't actually prove that in any way, shape, or form. You're saying that during the process in this you didn't report this to the Privacy Commissioner because you have all the information. Like, this is just incredibly negligent on your part, in my opinion, that you didn't go to the Privacy Commissioner because you considered that you have all the information. It's just ludicrous.

Dr. Abbott: NorQuest College followed the guidelines of the office of the Information and Privacy Commissioner. We had secured the data. We worked directly with the two employees that were impacted. As a result of what we did, we were able to ensure that information was secured. In fact, we were able to uncover an alleged fraud. So we believe that we handled things very well. Hindsight is always 20/20, but we do believe that this is an example of something being very well managed.

The Chair: Eight minutes for members of the government.

Ms Renaud: I understand that NorQuest wasn't legislated to report the breach publicly. Even though it wasn't legislated, you know, you've mentioned that legal counsel, EPS, the advice that you were given was not to report or contact or share information. But we've heard that there are several NorQuest employees who have had their personal information compromised, and they were not informed by NorQuest. In fact, the way that they found out that this was happening was through articles or information on either CBC live or on their website. So there clearly is a discrepancy. I'm wondering if you can speak to that. You know, was that an acceptable risk? Was that an acceptable action?

Dr. Abbott: NorQuest College followed the advice of our legal counsel and experts through the entire process. If you think about a postsecondary institution, our role is serving students, creating programs, working with our community to ensure that learners are well prepared, so we needed to go and get legal advice and get expert advice. We took the advice of legal experts in this process. The searches have confirmed that there was low risk of harm, so the advice that we got around low risk of harm in fact bore itself out as we looked at the data. Again, there were no social insurance numbers, no medical information. None of that highly sensitive information was contained there. We have followed up with all employees and specifically with those employees that had concerns, either those that came to my office and asked to meet to discuss it or those who went to the OIPC.

Ms Renaud: Okay. Thank you.

The Chair: Mr. Malkinson.

Mr. Malkinson: Thank you, Mr. Chair. I'm just going to following up on sort of the line of conversation that Mr. Taylor was talking about earlier. He was talking about some questions about, you know, whether all the data had been recovered from the individual and how the data breach seemed to have focused on two individuals. That was sort of my understanding of the back and forth that just happened there. My question is about: often we hear about how when there's a data breach, sometimes there's a lot of auxiliary data that comes when somebody is maybe pulling data out of a computer system for inappropriate purposes. Are you confident enough to state that the scope of the breach is limited to what's already been discovered and that there wasn't other data that may not have been the focus of the individual but came out with it, that you've already found all that data, that there wasn't even more information, and that there hadn't been other breaches during the same period?

Dr. Abbott: Based on the Anton Piller order, the securing of the data, the fact that we had experts review the data, we have confidence that we had contained the breach and that we have managed the situation. You know, we have no evidence to show us otherwise. It has been three and a half years, and there has been no evidence that the advice we got from legal counsel or the actions we took did not secure all the information.

Mr. Malkinson: Thank you.

I'm going to pass it along to Dr. Turner.

Dr. Turner: Thank you. I think, really, the most important question here is: what is management doing to ensure that fraud risk is mitigated on an ongoing basis in the college? Basically, I'm looking forward because it isn't just NorQuest; it's the whole college system that I think is at risk if there is any potential for what happened at NorQuest to be going on.

I do want to turn back, though, to what happened. I'm actually just completely amazed that the systems weren't in place to prevent this before 2012. You mentioned putting in systems like segregation of duties. That's a grade 3 system for management. Why wasn't that in place? Why did that individual that perpetrated the alleged fraud have sole-source purchasing? Who was responsible for not detecting it?

Dr. Abbott: First of all, I would speak to this specific alleged fraud. There was collusion involved. When there's collusion involved, it is almost impossible – you can have gold standard internal controls – to actually detect . . .

Dr. Turner: I'm going to just stop you for a moment. Why weren't those internal controls in place in 2012?

Dr. Abbott: I can only speak to the time that I got to the college, in 2010. I can tell you that . . .

Dr. Turner: Can I get Mr. Skoreyko to answer that, then? He was in charge in 2012.

Mr. Skoreyko: I'm sorry. I became chair in January 2014. I wasn't even on the board back then.

Dr. Abbott: Yeah. What I can tell you, though, is that when I came to the college, we had received feedback from the office of the Auditor General that we needed to improve our controls. We started working on a new project, an ICOFR project, to improve internal controls. I can't say that there was no segregation of duties before I arrived. I can tell you that there was some segregation of duties, but they needed to be enhanced. I think that when I look at the learnings that we've had, one is that organizations need to build an environment of continuous improvement around internal controls on the finance side and on the IT side. What we see is that IT is changing and finance is changing, so an environment of continuous improvement is always, always important.

Every time you get a new employee, you have to re-educate them on that. What we've really tried to do is develop this environment of continuous improvement because our world is changing. We particularly see that in the IT world. We have greater and greater demand from our students for mechanisms to do their studies. I

think something that all organizations are going to have to be diligent on is continuous improvement.

Dr. Turner: Thank you for that answer.

I have a question for Advanced Education, Mr. Skura. In the February 2012 and March 2013 Auditor General reports other postsecondary institutions . . .

The Chair: Thirty seconds.

Dr. Turner: . . . such as Athabasca University, Red Deer College, Olds College are listed as having concerns. Is the department satisfied that critical information systems in these entities are in place?

Mr. Skura: The short answer to that is yes. I mean, clearly with IT systems you constantly have to be monitoring as new threats become available, so we continue to work with institutions. We've really, from a department's perspective, been pushing greater co-operation amongst institutions, especially some of the smaller institutions. We have an organization, the Alberta Association in Higher Education for IT, that comprises representatives from my department and senior IT professionals from each college. The idea there is to get together and share best practices in some of these areas, so we are taking steps. You have to constantly remain vigilant on the IT front because they're always exposed to new fronts. We're paying close attention to that.

Dr. Turner: Thank you.

The Chair: Thank you.

Five minutes for members of the third party. I believe you were in the middle of a question.

Mr. Gotfried: Thank you, Mr. Chair. My first question is for you, President Abbott. From the hiring of Mr. Orleski in June 2007, it appears that there was an increase of his signing authority from $10,000 up to $25,000 and then in a subsidiary role up to $50,000. Do you now have procedures in place so that if somebody's signing authority is to be increased, there is a forensic process whereby you determine whether they are trustworthy?

9:30

Dr. Abbott: The first thing I would say is that NorQuest College has very good human resource processes in place. We do reference checks and criminal record checks. In fact, those were done on this particular employee. I think the bottom line is that we hired the wrong person, so that's tough. That can happen in organizations, where you hire the wrong person, and in this case something very significant happened.

With regard to signing authorities we have a suite of policies and procedures that outline how signing authorities are set and how they are changed. Generally as organizations get larger, you may have a change in signing authority because of the volume of transactions that would come to a particular manager. When we approve signing authorities, we review by position, we review by the level of authority someone might have, and the signing authorities are set. They are approved by executive and approved by the board of governors. So we do have good processes.

Mr. Gotfried: Thank you, Dr. Abbott. I think that's it on process.

I do have another question I want to get in. You also made reference to there being collusion. I guess, in my view, I would think it would be viewed that if it were collusion, it's hard and that under a general reference that collusion would be internal collusion. In this case it was external collusion unless there's something that we're not aware of here. External collusion is likely if there's going to be a situation like this. How can we protect against that external collusion, which is a likelihood in any of these cases, and use it as a justification for the fact that we didn't catch this?

Dr. Abbott: Yeah. I think that through our updated financial policies and procedures we built in some mechanisms. Our procurement process requires that for a purchase of $1 to $10,000, people are recommended to get some quotes. Anything over $10,000 requires three quotes so that we ensure that we are getting the right purchase and the right range of costs. Anything that is $75,000 or over goes out to RFP. Those mechanisms are there, and I think that they help to safeguard against what you're talking about.

Mr. Gotfried: Okay. I would hope that that process will work in the future.

I have one question for the deputy minister with respect to section 13(1) of the Financial Administration Act. There is a requirement in there that if confidential information subject to legal restrictions is disclosed to you, you also are bound by that. I guess my question here is: even if you can't disclose that information, have you received all the information you require with respect to the settlement so that at least we know that that is being administered and that any learnings from that can be addressed within your department, if not disclosed to the public?

Mr. Skura: Yes. Dr. Abbott and I and the institution have had several conversations about this settlement. As far as the department is concerned, we're comfortable that we have sufficient information on this.

Now, to your point on lessons learned, though, I mean, that's something that Dr. Abbott and I have been talking about. We have a number of tables with all postsecondary institutions where we're going to bring the lessons learned from this forward. The presidents of all institutions meet at least on a quarterly basis, so we'll certainly bring something forward to that but also to the IT professionals, that I mentioned before, as well as the senior business officers.

Mr. Gotfried: I have one quick question, then. Can you disclose to us whether the information has been disclosed to you or not? We realize that you can't disclose the details, but have they been disclosed to you, and can you disclose that to us?

Mr. Skura: I have sufficient information from NorQuest.

Mr. Gotfried: Okay. Thank you.

The Chair: You have 15 seconds.

Mr. Gotfried: I'm not going to try to squeeze one last one in.

The Chair: I've seen you try.

All right. We're now on to our second round of five-minute rotations, so the Official Opposition.

Mr. Taylor: We're going to give this over to Mr. Barnes.

Mr. Barnes: Thank you all for being here today. I appreciate it. I want to go back to 2012, and I want to talk about the culture and the internal controls. I'm looking at the Auditor General's summary here, that the college had 10 outstanding recommendations at the end of the fiscal year. Mr. Skoreyko, I'd like to ask you as chair: have you reviewed the culture that at the time might have led to this breach and this fraud? The fact that 10 – 10 – recommendations were outstanding. Briefly, can you explain what the culture might

have been at the time and how you're ensuring that this isn't going to happen again?

Mr. Skoreyko: If your question is with regard to the culture of the board, I can answer the question.

Mr. Barnes: Yes, please.

Mr. Skoreyko: The board back in 2012 – and I was a board member at that time – was fully informed of what was happening with regard to this. In April 2013 I actually sat in the gallery at Public Accounts when the 10 issues that were brought up by the Auditor General were discussed at the meeting. I was not a member of the Audit and Finance Committee, but as a member of the board we were carefully scrutinizing with Dr. Abbott at that time how we were to address those particular issues. I think that we have now concluded all of those issues since 2012 in a suitable manner.

Mr. Barnes: Okay. Thank you.

If I could ask Mr. Skura about the department's involvement in ensuring that the institutions are on top of the Auditor General's recommendations and ensuring that the culture is correct to ensure that we have best practices going forward.

Mr. Skura: Yeah. I'll answer that with a number of things. First and foremost, the expectation of our department is that all of our institutions comply with legislation and have adequate processes in place for internal controls. I think the issue of good governance starts with effective boards. It begins with recruiting boards with the right competencies. It involves providing board members with the necessary guidelines. It's ensuring that the boards have the appropriate subcommittees in terms of finance and audit committees that have the oversight.

In 2013 and 2014 the department did run some training for board members on the Audit and Finance Committee that was contracted through the University of Alberta. So we take that responsibility very seriously.

I mentioned a little bit earlier about the sharing of lessons learned. This is something that on a regular basis we certainly do through the groupings. The presidents get together with the department and the IT professionals as part of the AAHEIT group, that I mentioned before, the Association in Higher Education for IT, and the senior business officers get together as well.

Government is launching phase 3 of the agencies, boards, and commissions review. The scope of that review is still going through the government approval process right now, but one of the things that we are certainly looking at as part of that is a section on governance excellence. There we'll look at best practices: are there areas where we can improve the governance relationship between government and the boards and the boards and their institutions?

Mr. Barnes: Okay. Thank you.

Mr. Skura, are you confident that this college and other colleges are using best practices? We saw some stuff in the media last week about the processes of hiring, processes of remuneration. Again, it's my feeling that it's incumbent on your department to ensure that Albertans are getting the best value but to ensure that the process is transparent and the process is fair. Any thoughts, please?

Mr. Skura: Yeah. I couldn't agree more that it is incumbent on our department. That's what we're here for. We are taking steps on some of those issues that you mentioned. On the issue of, you know, the ABC review it will look at more than just governance excellence. Again, that's still going through the government process, but there will more than likely be an examination of compensation as part of that. We are constantly working with the institutions. We have governance processes in place. We require every institution to submit an institutional plan every year from an annual report perspective, and we take that very seriously in terms of following up. So we do have governance processes in place.

9:40

The Chair: Thank you.

Five minutes for members of the government.

Ms Miller: Thank you, Chair. Mr. Skura, the government of Alberta has committed to board renewal and a new transparent appointment process. Good governance is required to prevent situations such as the breach of privacy at NorQuest. What work is being done by your department to support boards to mitigate these kinds of risks?

Mr. Skura: Thank you very much for the question. As I alluded to before, we've launched a much more robust process around recruiting. Good governance, I believe, starts with having the right board members with the correct competencies to oversee board governance. We're going through that process right now. A number of new appointments are following the new process. The net has been cast much wider now in terms of the recruiting process.

As I mentioned earlier, we conducted some training in 2013-2014, and it will certainly be something that we'll be looking to as part of that governance excellence piece that I spoke to as well to make sure that board members have the appropriate training.

Again, I think governance also applies beyond just the boards. As I mentioned earlier, having those tables where key management staff from each of the institutions can gather together, share lessons learned, share best practices is very critical to moving forward and having a totally effective governance and management process in place.

Ms Miller: Thank you.

Mr. Dach: Thank you, Mr. Chair, and thank you to all participants for treating so seriously the matters that we're talking about today. Fraudulent activity and security breaches are a concern for all organizations. Be they private or public, they are subject to continuing risks of fraud and misappropriation. To the department members: are you able to tell me if there are government-wide rules in place that need to be updated to prevent these types of situations?

Mr. Skura: As I mentioned before, we expect the boards of each of our institutions to put policies and processes in place to manage the risks at those individual institutions. From a department perspective we'll monitor to make sure that there are appropriate policies in place. Again, we have really been pushing the co-operation amongst the institutions as well as far as lessons learned.

I will also say that in November of this year there was a conference held that was jointly cohosted by this AAHEIT group that I talked about and its sister group from Education. The idea was to get senior IT folk together and discuss the latest threats and issues facing the IT community. So, yeah, we are actively involved in terms of making sure we're addressing those risks.

Mr. Dach: Thank you, sir.

I'll hand it back to MLA Miller.

Ms Miller: Another question. In today's world ransomware attacks are becoming an increasing problem. In the summer of this year the University of Calgary paid $20,000 in ransom following a cyberattack on its computer systems. What is the department doing to protect Alberta taxpayers from having to pay for release of data?

Mr. Skura: Thank you very much for that question. Again, as part of this conference that I referenced, that happened in November, both NorQuest and the University of Calgary participated in that, and part of the discussion around that was how to deal with ransomware requests. We also had participation in that conference from the senior information officer from the government of Alberta, so there was discussion there in terms of highlighting what best practices could be in terms of dealing with those. These issues are complicated. I don't have the details with me today on the University of Calgary, but certainly there are lessons learned from that as well, that the University of Calgary is looking at and we're looking at from a system-wide perspective.

Ms Miller: Thank you.

The Chair: Are you finished with your time? Okay. Thank you.
Five minutes for members of the third party.

Mr. Gotfried: Thank you, Mr. Chair. Just a couple of questions here with respect to the situation. I guess I can maybe sort of put them together, and you could respond to them, Dr. Abbott. Does the ministry have full information about why the alleged perpetrator of the fraud and harassment was terminated and the HR records to address that? And my second, somewhat related, question is: if Mr. Orleski had not begun the alleged harassment and the evidence had not been seized from his residence or if it had been destroyed, do you believe that NorQuest would have uncovered the alleged fraud or pursued the alleged fraud or breach of public trust in such a manner as to be able to pursue it and get some recourse in terms of the financial damages done?

Dr. Abbott: With regard to the former employee, management was managing the performance of that individual starting really from the summer of – I've just got to get my dates right – 2012. So we were managing that. That is typical in any postsecondary organization that is board governed, that management would manage that. Certainly, hindsight is 20/20 in terms of when you release an employee, and there's an appropriate severance that goes with that. We weren't aware of the alleged harassment at that time. So, really, if there is anything that could be done over, if we knew that, there certainly would not have been a severance paid out to that employee. This was managed in the day-to-day running of a postsecondary institution.
Could you repeat the second part of the question for me, please?

Mr. Gotfried: Actually, I've got a supplementary to the first one, which is: was the employee's termination, any of that, related to financial irregularities that may have been uncovered already at that point in time?

Dr. Abbott: I think it's identified in the court documents. There were challenges with the individual not following our policy around mobile devices. The issue relates to a large phone bill that we received, so that's really where that started. Then the individual was not following the instruction of his supervisor. That's really where it started.

Mr. Gotfried: Okay. The second part of the question was: had the harassment not begun – so, I guess, the forensics into the alleged harassment, breach of data, and thereby the information that was found about the fraud that was perpetrated – do you believe in your heart of hearts that any of that would have been uncovered had he actually been more prudent in his fraud and kept his mouth shut?

Dr. Abbott: That's a very difficult question to answer because it's hard to say. It's really hard to speculate. It's kind of the reverse of: hindsight is 20/20.

Mr. Gotfried: Absolutely.

Dr. Abbott: I don't really have that crystal ball, so I think it's very hard to say.

Mr. Gotfried: Okay. Just another question with respect to some of the privacy legislation. We've talked a little bit about the disclosure and the delayed disclosure of the information. Again, I'm assuming that because of the nature of your public institution, it would be treated similarly to a nonprofit organization, and you're not actually subject to the office of the Information and Privacy Commissioner, to the full PIPA. Is that actually the case? What are your thoughts on whether that should be the case, perhaps, in the future? We've been reviewing that piece of legislation in another committee I sit on as well.

Dr. Abbott: Okay. I'll let Joan respond on the PIPA side.

Mrs. Hertz: Right. We are not subject to PIPA, but we are subject to the Freedom of Information and Protection of Privacy Act.

Dr. Abbott: And I would say that overall we take having private information very, very seriously. I think the guidance we get from the office of the Privacy Commissioner is very solid, and I can tell you that our employees who have this as a delegated responsibility speak to the Privacy Commissioner often. There are often learnings that come from that. So I think that overall we are sitting in a good position. The communication between parties is always very positive, and the learnings are shared through memos and bulletins that come out.

Mr. Gotfried: All right. Thank you.

9:50

The Chair: Thank you.
I'll thank officials from NorQuest College [An electronic device sounded] and the Ministry of Advanced Education – school is out – for their presentations today and for responding to committee members' questions. We ask that any outstanding questions be responded to within 30 days and forwarded to the committee clerk.
I'll briefly offer an opportunity for members to read written questions into the record, without preambles or statements.

Ms Miller: What are the processes in place for department officials to brief the minister when issues take place such as the ones discussed this morning?

The Chair: Any others? Mr. Taylor.

Mr. Taylor: Thank you, Mr. Chair. I would like to ask the Auditor General if he thinks there are ways that this could have been prevented?

The Chair: Any other questions?

Mr. Gotfried: I'd like to ask if NorQuest College or the ministry feels that the postsecondary institutions should be subject to the full PIPA legislation?

The Chair: Mr. Barnes.

Mr. Barnes: Thank you. I would like to ask the Department of Advanced Education if they're satisfied that NorQuest has made all

necessary public disclosure of the alleged fraud and privacy breach and if they are satisfied with the controls they've implemented to ensure that this won't happen again?

The Chair: Last chance.

Are there any other items for discussion under other business?

All right. With the agreement of the committee, the committee working group will determine the invitees for an out-of-session meeting anticipated for a date in January, to be circulated to committee members for review and approval. A full proposed spring 2017 meeting schedule will be assembled by the committee working group for consideration by the committee at that out-of-session meeting. Are members in agreement with the out-of-session meeting? Yes? Okay.

This concludes Public Accounts for fall 2016. I'll call for a motion to adjourn. Moved by Mr. Malkinson. Any discussion? All in favour of Mr. Malkinson's motion to adjourn? Opposed? On the phone? Carried.

[The committee adjourned at 9:52 a.m.]

Published under the Authority of the Speaker
of the Legislative Assembly of Alberta