M12600

NOVA SCOTIA ENERGY BOARD

IN THE MATTER OF: ***THE PUBLIC UTILITIES ACT***

- and -

IN THE MATTER OF: **AN INQUIRY** about the impact of the cyber incident on **NOVA SCOTIA POWER INCORPORATED's** collection and retention of customer information, customer service and communications, billing processes and regulatory matters

---

TRANSCRIPT

HEARD BEFORE: Mr. Stephen T. McGrath, K.C. Chair
Mr. Roland A. Deveau, K.C., Vice Chair
Mr. Richard J. Melanson, LL.B., Member

PLACE HEARD: Offices of the Nova Scotia Energy Board
1601 Lower Water Street, 3rd Floor
Halifax, Nova Scotia

DATE HEARD: Wednesday, August 19, 2026

APPEARANCES:

APPLICANT: **Nova Scotia Power Inc. (NSP)**
Mr. Colin J. Clarke, K.C.
Ms. Jennifer Power, Counsel
Mr. Geoffrey Breen, Counsel

INTERVENORS:	**Consumer Advocate** Mr. David J. Roberts, Counsel Mr. Michael Murphy, Counsel
	Small Business Advocate Ms. Melissa P. MacAdam, Counsel Ms. Rebekah L. Powell, Counsel
	Formal Intervenor, Mr. David MacLeod Ms. Elisa Akcakiryan, Counsel Mr. David MacLeod
	Industrial Group Ms. Brianne Rudderham, Counsel Mr. Isaac Cain, Counsel
	Nova Scotia Department of Energy Mr. Thomas Kayter, Counsel

BOARD COUNSEL:	Mr. William L. Mahody, K.C.
BOARD STAFF:	Mr. Somesh Singh Mr. Robert Norwood, Public Proceeding Assistant Ms. Svitlana Lykhina, Public Proceeding Assistant Mr. Jordan Long, Information Systems Technician
RECORDED and TRANSCRIBED BY:	**INTERNATIONAL REPORTING INC.** Ottawa, Ontario

I N D E X O F P R O C E E D I N G S

I N D E X O F P R O C E E D I N G S

LIST OF EXHIBITS

LIST OF UNDERTAKINGS

LIST OF UNDERTAKINGS

LIST OF UNDERTAKINGS

Halifax, Nova Scotia

--- Upon resuming on Wednesday, August 19, 2026 at 9:01 a.m.

THE CHAIR: Good morning, everyone. Any preliminary matters before we start back up again?

Mr. Mahody.

MR. MAHODY: Thank you, Mr. Chair. Good morning.

GLEN MacLEOD, Previously Affirmed:

CHRIS LANTEIGNE, Previously Affirmed:

LIA MacDONALD, Previously Affirmed:

BLAKE WILLIAMS, Previously Affirmed:

CROSS-EXAMINATION BY MR. MAHODY, (Cont'd)

Q. Good morning, witness panel.

I have just a couple of areas to address, and the first is in the rebuttal evidence, N-17, at page 18 of 65.

This is the section of the rebuttal entitled, "Additional Relevant Records, Section 3".

So if I could just move to the middle of the page, the December 2024 privacy audit of Data Lake, I just want to confirm -- and Nova Scotia Power's been clear as to why it's putting this information in here, but you agree that the technical aspects associated with the Data Lake, its audit, how it operated, how it was accessed will all be matters for the compendium cyber matter.

A. (Williams) Absolutely, sir. Yes.

Q. Thank you. All right.

So just moving up to the top of the page, then, about the retention schedule and Personal Information Inventory, I just wanted to confirm that the Personal Information Inventory that's attached to your rebuttal affidavit as confidential Attachment 3, that's the first time in this proceeding that that Personal Information Inventory had been put on the record. Is that correct?

A. (Williams) Yes, that's correct.

Q. Okay. And the purpose of the Personal Information Inventory is for Nova Scotia Power to identify what personal information it holds and where it is stored. Is that correct?

A. (Williams) Yes. At a high level, sir, yes.

Q. And obviously, the attachment itself is confidential, but there are references in the -- each of -- in that confidential attachment to the last

update for the documents that are provided for. I won't get into the dates that are there.

But I take it that this is the Personal Information Inventory as at April of 2025. Is that correct?

Time of the attack, I think is what the evidence is.

A. (Williams) Yeah, that's accurate.

Q. Mr. Williams, just on that point about the time of the attack, some reference in the rebuttal evidence as well to potentially some customer confusion about when Nova Scotia Power became aware of the intrusion.

You do agree with me, though, that customer reaction would be impact -- would reasonably be impacted by the time as when Nova Scotia Power indicates it was first exposed. So the March 19th date becomes a relevant concern to customers given the personal information that was exposed.

A. (Williams) So just a couple parts to that question, I think.

So it's not a relevant date in terms of information being exposed. It's a relevant date in terms of the attack and when the threat actor gained access to the system. But -- and this will be explored further in the other proceeding you're referring to, but they did not access the data we've been discussing in this process on March 19th. That did not occur until April 25th.

But to your point, I think, sir, the existence of two different dates, one being demonstrated by the discussion you and I just had, there's some nuances to the March 19th and the April 25th and what happened on those two dates, so I certainly understand why the fact that there is those two dates would create some confusion for people.

Q. Do I take it from that response, then, that the first time that the threat actor gained access to personal information was on April 25th?

A. (Williams) So that is something that I think needs to be more precisely confirmed as part of the next, but it was not March 19th. It would have been April 25th or thereabouts, yes.

Q. But again, all of the technical issues associated with that 37-day dwell time period that the third-party intruder had at Nova Scotia Power's system will all be matters for the other cyber matter.

A. (Williams) I would agree, yes.

Q. Mr. Lanteigne, I had a question about utilizing photo meter reads. And based on the pre-filed evidence, and I think your testimony as well, I understand that photo meter reads became an acceptable method in about November of 2025.

A. (Lanteigne) Yeah. And to just clarify that -- and I hope I said it yesterday, and if I didn't, I apologize -- but the -- we would accept photo reads through our customer care team in the months leading up to November as well. So we would use them to resolve

situations in talking to customers where the meter read would obviously help resolve that situation.

It was in November that we actually added the online form to the website for customers to be able to submit the photo reads.

And just after conferring with my colleagues, they've reminded me that, you know, accepting a photo read is an established part of our regulations as a way to update a customer's bill charge.

Q. Sure. But in November 2025, you revised your mechanisms to make it more straightforward, more streamlined for photo reads to be submitted in the place of a meter read. Is that correct?

A. (Lanteigne) Yeah. Essentially, we scaled up that activity with the online form to allow customers to take advantage of that option.

Q. Now, some may look at a -- the period between May 2025 and November 2025 as being a lengthy time to get that initiative up and going. What do

you say to that?

A. (Lanteigne) I think from my perspective, again, it's important to note that, you know, we were able to process them in the time between June, I guess, when billing resumed and November. And our team would do that if a customer called in. It wasn't to the volumes that we had after November.

I think, again, what I'd mentioned yesterday was that our focus was on two things. That was, you know, obviously estimating bills, which we've talked about extensively in this hearing, and also securing meter readers to actually read meters for customers. Again, based on the length of time that we had had to estimate bills, it was in November that we made that determination to add the option to our website for our customers.

I think as well, to accept those at that scale and volume back in June and July, you know our teams would not have had the ability to process that volume that was actually coming in as well. We needed to

get to the point in November where it was possible.

And finally, I think one of the pieces I touched on yesterday that's important to reiterate is, you know, in the month of December, for example, we did -- we made about 500 adjustments to accounts based on photo reads. We did estimate about 157,000 bills in the month of December. So while we wanted to make sure that option was there for customers, and we felt that the timing was right to put that functionality online, there was not a significant uptake, but we were glad to provide that option for any customer who wanted to take advantage of it.

[9:10:29] **A.** (Williams) Again, Mr. Mahody, I would just add to that. I think what that demonstrates for us, I think, is that we appropriately prioritized the mechanisms we had available to us. Had we proceeded with prioritizing photo meter reads, rather than getting meter readers out into the field, I think we would have had a very different and less favourable result than we actually

did in terms of what we were able to read on actual meters.

Q. In your testimony yesterday, Mr. Lanteigne, you mentioned customers responding to the photo read option by the fall of 2025 with responses like, "That's your responsibility, Nova Scotia Power, not mine, to read the meter. You can get someone out here to do it." Do you recall words to that effect?

A. (Lanteigne) That is correct, yes.

Q. Yeah. Is it the case, though, that having deferred the real utilisation of photo reading until November, you deferred it into a period where customer relations were strained by that point?

A. (Lanteigne) I don't take that premise, no.

Q. Such that you would view the reception of photo read to have been the same, whether it had been -- whether what was initiated in November had been initiated in June, your understanding is that it

would be a similar response take-up rate.

A. (Lanteigne) I can't speculate on that. You know, again, to what Mr. Williams said, I think our -- you know, I think our approach to supporting our customers throughout this incident has evolved, and it's been based on feedback from customers and stakeholders. You know, again, I think our approach to focus on meter reads, and also on estimated billing, where we weren't able to obtain a meter reader, like that was the approach that we took, and I think that resulted the best possible results we could have had throughout this incident.

And I think the other issue that emerged with photo reads as well, I discussed the -- like, the volumes that were coming in against the estimated bills. We actually found that about a third of the submissions that were received for photo reads were actually on accounts that did have true reads. So adding that third layer in again, we were doing it right from the start reactively if a customer needed that support. We

scaled it up based on the evolving feedback that we were getting from our customers. And again, the uptake was not high, but we were happy that that option was there when we did put it out in mid-November.

Q. Thank you.

MR. MAHODY: Thank you, Mr. Chair. Those are my questions.

MR. CLARKE: Thank you.

Mr. Melanson.

MEMBER MELANSON: My microphone is a little far away from my computer, so I'm just wanting to make sure that my sound level is okay, Mr. Norwood.

MR. NORWOOD: Yes.

MEMBER MELANSON: Okay.

QUESTIONS FROM MEMBER MELANSON

Q. Let's start. My first question, I'm going to turn to Exhibit N-17.

MEMBER MELANSON: And it's PDF page 10, Mr. Norwood, and at lines 25 to 27.

BY MEMBER MELANSON:

Q. And it says, and this is elsewhere in the evidence, but this is the rebuttal evidence where it says, "At the time of the Attack..." Sorry. It says:

> At the time of the [cyber incident of] NS Power...cybersecurity standards and policies that [were] informed, in part, by the...(NIST) Cybersecurity Framework...

So informed in part. And I just -- now, without getting into the NIST framework and what entails, at a high level of governance issue proportion, do you know why the entire NIST framework was not incorporated at the time?

A. (Williams) I, unfortunately, don't have an informed response for you, sir. I think

it's certainly a reasonable question to ask, but it would be better asked to the panel that would appear as part of the, I guess, Mr. -- the compendium proceedings, Mr. Mahody referred to it as.

Q. Okay. The reason I ask it is, there's a response in Exhibit N-11 to the SBA IR-13.

MEMBER MELANSON: It's PDF page 25, Mr. Norwood in Exhibit N-11.

MR. NORWOOD: What page is it?

MEMBER MELANSON: Sorry. PDF page 25.

BY MEMBER MELANSON:

Q. And here, it's referring to a portion of the incident report, but it talks about, "In connection with these efforts..." -- this is the question:

> ...NS Power has recently completed an extensive two-year update to its cybersecurity practices to comply with current policies and anticipated changes in [the] standards communicated by NIST.

And the question is, "When was the two-year update completed?" And the answer is, it was

concluded:

> ...concluded its two-year update of...cybersecurity practices spanning 2023-2024, with [a] formal closeout on February 3, 2025.

My question is, it seems like in this answer the NIST framework was being used at the time of the entire NIST framework, and anticipated changes was being used at the time of the cyber incident. I'm just wondering if there's an explanation. It was or it wasn't, I think is the question.

A. (Williams) So again, Mr. Melanson, and I apologize, but I know this is on the record in this proceeding, and we've answered it attempting to be responsive and transparent, but this panel's not going to be able to speak in detail. I would say that it would certainly be my understanding that NIST, as your basis and your guidelines, that there would be other guidance materials and other external factors that would inform the cybersecurity posture of Nova Scotia Power.

Q. Okay. I mean, certainly I realize there's going to be an expert report for the other proceeding, but it was on the record and ---

A. (Williams) Absolutely.

Q. --- it's slightly inconsistent in the two provisions.

Okay. I'm going to go into another issue that may have the same result. But there is, in the incident report, that's N-16, and I'll go to the reference, and again it may be for the other proceeding, but I don't know if you can speak at it at a high level. It's N-16, PDF page 40. Has to do with NERC standards.

And it talks about, at line 6 and 7:

> Regarding security audits, NERC conducts extensive periodic audits (including security) of the Company's Energy Operations to ensure effective compliance.

And my simple question was, the NERC standards, as I understand it, would not necessarily result in audits of the IT systems surrounding the

operating system. Am I correct about that?

A. (MacDonald) Yes, it's more focussed on the OT grid management systems.

Q. So that NERC audits would not necessarily be looking at IT systems when they're doing their audits through the Northeast Power Coordinating Council?

A. (MacLeod) There's a little overlap into the IT realm, things like network controls and firewalls, which could be servicing IT or OT purposes. But as Ms. MacDonald said, the intent is to cover the OT grid management technologies with those NERC audits.

Q. Okay. Going to turn to bill estimation. And just for basic understanding, with the AMI system, bill estimation is done through that system; correct? You don't have to rely on the CIS system?

A. (Lanteigne) That is correct.

Q. And just for my own knowledge, in what circumstances would there be estimated bills under

the AMI system? I would have thought there probably wouldn't be unless the system is down.

[9:19:56] **A.** (MacLeod) There can be times, for instance, if there's a power outage, that could be local power outage due to a vehicle accident or a larger storm-related power outage, some of the AMI equipment may be down for a short period of time. And if that customer's bill cycle were to occur at that time, there could be some missing reads.

Q. Okay.

A. (MacLeod) So the AMI system will do its best to estimate what might be missing to pass that along to billing.

Q. Okay.

A. (Lanteigne) Sorry, could I just add to that, Mr. Melanson? I think the key piece about -- what Mr. MacLeod said, he's absolutely right; Nova Scotia Power maintains a billing cycle for a customer. So if one of those incidents that he described occurs on a date

where bills are supposed to be issued for a customer, that would result in it being an estimate because the approach is to not delay the issuance of bills if we can avoid it and to help provide a predictable schedule for our customers. I just wanted to add that; sorry to interrupt.

Q. No, no, it's fine. And that in many ways explains from a performance standards' point of view, that there wouldn't be a whole lot of these instances that would occur; correct?

A. (Lanteigne) In normal operations, Blue Sky operations per se, they're infrequent and the performance standard is what we keep our eye on for sure around managing.

Q. Yeah.

THE CHAIR: Just in terms of the estimation that may occur in those situations, am I correct that because the AMI system is feeding data back to the central systems more or less constantly, that the period of estimation would be fairly short if there was a

momentary outage at the time of the billing cycle?

MR. MacLEOD: For most cases, yes. If -- in a typical customer a bill cycle might be a 60-day bill cycle, we may have 52 days of daily reads and then the estimation would be for that final eight days. So depending on -- there are some circumstances where it could be longer but generally that's how it works.

THE CHAIR: In what circumstances would it be longer?

MR. MacLEOD: If there was something happening at the customer premise that needed a major repair, or a home business, but for the most part it's fairly small windows that need to be estimated.

THE CHAIR: Thank you.

Sorry.

BY MEMBER MELANSON:

Q. So the use of the CIS system really is a situation where you have, as we have here, a prolonged and major impact on the ability to obtain AMI

data; would that be fair?

A. (Lanteigne) That is correct. So the CIS estimation routine would be used in two circumstances; the one would be a continency if the AMI estimation is not available, again, in absence of an actual true reading for the customer's account. And the second instance would be if a customer has opted out of an AMI meter and that bill needs to be estimated, the CIS estimation routine would be used in that circumstance.

Q. I can't remember, I should know this, but how many -- what the percentage of opt-outs is for customers?

A. (Lanteigne) I think it's about 3.5 percent of our customers, yeah.

Q. So if something happens with respect to your not being able to obtain true reads from that 3.5 percent of customers, the CSI system has to be used in that circumstance?

A. (Lanteigne) That is correct.

Q. Okay. But before AMI the CIS system was used for all bill estimations; correct?

A. (Lanteigne) That is correct.

Q. So there would have been a long history of using CIS for bill estimation before the cybersecurity incident happened?

A. (Lanteigne) That is correct.

Q. I might as well just bring it up; I think it's been discussed at length as to what the actual process is, but let's take Exhibit 10, IR-1(c).

MEMBER MELANSON: I don't have the PDF. IR-1(c), the response to IR-1(c). You may have already gone by it. There. Keep going, keep going. Keep going, after all these bills. There.

BY MEMBER MELANSON:

Q. How I understand it, the estimate is a reading doing the average usage search per day at a specific property on bills in the last 12 months that considers it the same season. So in other words, you're

looking at a 12-month period for the same property but based on season; is that correct?

A. (Williams) That is correct. And I think one of the pieces that I talked about yesterday is the seasons, they do not follow the same, you know, four seasons that we experience in Nova Scotia. CIS would consider two periods of time, so the warm season and the cold season.

Q. Right. And it's based on bills that are issued in those two seasons, past bills that are issued in those two seasons; correct?

A. (Williams) That is correct, yes.

Q. And there is no ability to track a daily amount; it's actually an average amount that's used for the billing period?

A. (Williams) That is right; your understanding is correct.

Q. Yeah. So that, for example, in the November bill, for the first bills in the cycle in

early November, it would incorporate data from September, for example?

A. (Williams) Yeah, that's correct. I think in November the specific feedback that we had from our customers is that as seasons transition, because November would have been the first month of the colder season ---

Q. Right.

A. (Williams) --- and what we had talked about yesterday was that in the first few weeks of that month, that is where we recognize that some of the estimates -- again, what the CIS system was doing was providing the average daily cold usage for the customer, but it -- you know, coming in at the start of November it would have been -- you know, for some customers, it would have been a higher estimate than they would have been expecting.

Q. But isn't the reason for that because you have -- in that cold period, you have, let's

say, information from September, for the first billing cycle in September, October, November -- or sorry; October, November basically?

A. (Williams) That is correct. So the period of time that was being billed against the colder weather usage did cause some of those estimates in the first few weeks (inaudible due to mumbling). You're right, yeah.

Q. And just actually to make sure I understand this, is it actually that or are you -- when you do the per -- the average daily usage, are you using the entire six-month period from -- for that billing, for that cold weather season? In other words, are you taking -- when you're billing in November, are you also taking data from December, January, February, March?

A. (Williams) Yeah, essentially the Customer Information System's estimation routine would use the date of the bill to determine the season for the period of time.

Q. But they would use the average daily use for the entire season?

A. (Williams) That's correct, yes.

Q. So that they're incorporating the temp in March, January, February data into the November bill?

A. (Williams) That's correct. And what we talked about yesterday, like, when the season can change, whenever the season does change I guess -- again, not traditional seasons but warm to cold or cold to warm, that's where the average daily usage, you know, can cause an estimate that is off.

Q. Yeah. So you essentially have data, combined data, agra-data for three billing cycles for most residential customers that we can take an average for that entire period; correct?

A. (Williams) Yeah. Essentially with it being split into two periods of time that are assessed, the average customer would get six bills a year,

yes.

Q. And it's not based -- because if a customer -- if a new customer enters into the premises during that estimation period, there's no way of adjusting the average to account for a different -- for usage and that type of thing for a new customer, for example?

A. (Williams) That is correct. So the premise history would be used for the estimation, and I think the example I provided yesterday, if a home had a single person living in it and a family of five moved in, obviously that usage profile could change from that, or any other changes that the customer may have made in their home; if they heat with electricity now, whereas they heated with oil in the previous period, those types of determinates would not be something that we could include in the estimation.

Q. And there's no way -- am I right that there's not a mechanism whereby employees can actually get into the system and change the output? The

output is the output from the system.

A. (Lanteigne) I think -- and just building on what -- the discussion that I was having with Mr. Mahody earlier as well to, you know, recognizing at the beginning of November some of the changes that occurred, that was one of the -- one of the reasons that I mentioned evolving kind of customer and stakeholder feedback that we were receiving while we wanted to kind of increase the promotion of the photo meter read option, so providing that option for customers to allow our customer service associates to actually get the meter read to make the changes that you are talking about to actually be able -- but other than that, you are correct. We're not able to apply, like, a change to that estimation routine across the entire Customer Information System.

[9:30:14] **Q.** So when a suggestion was made that somehow the bills were being manipulated to be higher, in fact, the system produced the bills that you were generating. Is that correct?

A. (Lanteigne) That is correct. There was no manipulation of bills at all.

Q. And basically, the CIS subroutine that's used as a backup in this situation, that was never intended to be used over a lengthy period of time. Is that correct?

A. (Lanteigne) You are correct.

I think the -- you know, again, as Mr. MacLeod described, and we were talking about earlier as well, we do know that we've evolved the estimation for AMI meters, and that's what our primary approach was. And even for opt-out customers or pre-AMI, the intent of Nova Scotia Power is to get out and read customers' meters every bill. So the period of estimation, as I talked about it yesterday, I think is what compounded the problem and the concerns for customers.

It wasn't just the one estimation. It was that they might have had multiple ones in a row and then specifically when those true reads occurred, you

know, if -- especially if a customer had been under-estimated, as I talked about yesterday, or they had underpaid or seasonal usage drove the impact, that that definitely caused concerns for our customers that we've been supporting them through.

Q. And when you talk about the multiple estimated bills, in fact, in that scenario would not the CIS system produce results -- the second estimated bill or a third estimated bill might be replaced on a previous estimated bill?

A. (Lanteigne) You are correct. Like, multiple estimates in a row would -- could potentially drive that scenario. I think for -- from our perspective, the timing of the restoration of the AMI and then getting back to the point where we were getting true reads, it meant that CIS was still able to look at actual data from the year before, so true reads from the year before, to make the determinants.

But you are correct; like, if that

estimation had to continue beyond the period that it did, you would have had timeframes or estimates for comparing estimates.

Q. Given -- I know there's discussion in the evidence about the new Customer Information System that's being planned and may come to the Board -- well, at some point if it's planned to come to the Board. But that -- I guess do you have any sense of when that application is going to be ready?

A. (Lanteigne) Our hope is that it would -- the application would come to the Board by the end of this year.

Q. And if that were to happen and if the application were approved, how long would it take -- do you have a sense of how long it would take to implement that system so it would be up and running?

A. (Lanteigne) Our belief at this time is that it would be approximately 2029 to implement, based on the timelines that we've considered.

Q. So between now and 2029, the current CIS system would be the backup and also used for the customers that opted out; correct?

A. (Lanteigne) Yeah. So currently, the AMI estimation routine would be the system for AMI customers. For the customers who opted out, if we needed to estimate bills, you know, the CIS system would be used.

I think it's important to note that, you know, since April we've had our -- you know, we've been reading customer bills again, we've been meeting the performance standard every month since April. And our -- you know, our approach is to continue to do that to try to minimize estimates because, as we've talked about and you've highlighted, I think it's the amount of estimates, multiple estimates in a row that really caused concerns for customers.

Q. And in reading the evidence, it appeared to me that there might not be very much done to the existing system to assist in making it more accurate.

Am I reading that correctly?

Leaving aside the change in the start of the ---

A. (Lanteigne) Yeah.

Q. --- cold season, but ---

A. (Lanteigne) --- Yeah.

Q. --- within the program itself.

A. (Lanteigne) Yeah. That is -- your understanding is correct. Making modifications to the Customer Information System is -- in this case, we do not believe it's possible.

Q. Not even -- for example, one of the things I was thinking of is with having a longer period like two cold weather seasons and two hot weather seasons as the basis for the estimate, is that at all possible, number one? And number two, would it change the outcome?

A. (Lanteigne) I appreciate your patience. I just wanted to double-check my understanding.

But no, the complexity of the estimation, it would not be possible in the system to change it.

Q. And looking at the cost that's estimated for the proposed new Customer Information System, and you talk about a three-year period, I suppose any interim solution that you would look at would have a cost as well beyond what you're using now? If there was one available.

A. (Lanteigne) Just to clarify, the project itself would approximately be a 24-month delivery upon approval from the Board. I think that's just important to note. And we don't believe that there would be a way with the existing Customer Information System to actually, I guess, come up with an enhanced or different way of estimating those.

And if I could ask Mr. MacLeod just to elaborate on that, I would appreciate that.

A. (MacLeod) True statement by Mr.

Lanteigne.

Just kind of goes back to the legacy system, and I'll touch on that. The risk -- the billing works as designed and produces accurate bills, and in a legacy system we just do not want to do anything that puts that in jeopardy, so that's why the legacy system we're taking very careful thought before doing anything inside the legacy system.

To move a billing function or a calculation -- a bill calculation somewhere else and bring it back in is also complex and risky. And keeping that customer account meter relationship and everything that goes with that and move-ins and move-outs, it's -- it's just not possible to do an interim step, so the best pathway is towards a new CIS system.

And to say for estimation specifically, we have AMI back in place. It is a robust estimating system, and anticipate that will be in place right up to our new CIS, beyond that as well.

Q. Well, I appreciate that you're not going to use the CIS system to do bill estimation except for that limited circumstance for those that have opted out. I'm just looking at if something happens in the interim between now and when the new GIS -- sorry; CIS system is put into place.

A. (MacLeod) With how we're architected in the cloud now, we have much more resiliency. The previous AMI system was at our local data centre where the threat actor in this circumstance -- that was one of the places that was affected by this cyberattack. With it being in the cloud, there's more resiliency and redundancy, so we ---

Q. So if ---

A. (MacLeod) --- don't expect ---

Q. --- if there were an incident and it's in the cloud, you might be able to access it, but you couldn't access it in this ---

A. (MacLeod) Might fail to access it

or bring it back to normal operations.

A. (Lanteigne) And to clarify as well on your concern for opt-out customers specifically, I think, again, we've talked about how multiple estimated bills in a row obviously exacerbated some of the concerns that were occurring, but the situation, if we still need to estimate a single bill for our customer, you know, our team is obviously focused on making sure that the next ones are true rather than having multiple bills in a row estimated, so it should help mitigate the concern as we leverage the current system.

Q. You mentioned a few times the fact that the majority of the concerns that have been expressed to NS Power relate not so much to the overbilling situation but the -- or the overestimation situation but to the underestimation situation where a large amount was outstanding. Is that partly due to the fact that because you reverted back to the warm weather subroutine, it created that problem?

[9:40:40] **A.** (Lanteigne) I actually -- I do -- I don't want to say that decision didn't result in some of them, but I think the concerns that I was referring to were actually concerns that existed even prior to November. So those were the customer escalations that were coming to us and concerns that were coming to us. That was what was causing the issue, was just that true read coming in, if it had been below because again something in -- in many cases, something changed at the premise to drive up usage in the customer's home. Those concerns were prevalent prior to November. So again, I don't want to speculate and say that it did not occur after November because of that specific issue, but I know that that was an issue that we were experiencing all along.

Q. One final question. I'll just make sure -- I'll ask the question and I'll check back to see if I have any other questions on billing.

MEMBER MELANSON: But N-17, in the

rebuttal evidence, and it's at PDF page 37 and flowing into page 38. So we can show, Rob, the bottom of PDF 37 and the top of 38 in N-17.

BY MEMBER MELANSON:

Q. Okay. So at line 28, starting at the sentence:

> If NS Power does revert to CIS estimated billing again, the Company has tracked lessons learned, has more detail regarding how to adjust seasonal logic further for accuracy, and will consider all reasonable efforts to become better equipped to handle volume and duration if the seasonal subroutine remains a secondary contingency.

I guess my first question on that is I didn't think that you could adjust the seasonal logic further than what you've already done, can you?

A. (Lanteigne) I think the lesson learned is exactly what you described and what we listed here in the evidence. I think the -- you know, the approach from our perspective is that if we were in a situation again where estimation had to happen at a high level heading across kind of the change of seasons in CIS,

heading into that, we would be able to potentially make minor adjustments to allow us to try to improve, again recognizing that estimates are estimates. But that's one of the biggest takeaways from that.

And I think that some of the other pieces that, while it's not CIS estimation routines specifically, but some of the items that we talked about yesterday was just how, you know, our AMI restoration efforts that have happened have included a more robust contingency plan to ensure that it's available and that we don't have a situation like we did last year where we lose that functionality from April until the restoration started in late December.

Q. You used the phrase again -- and I'm not sure if you said minor, but adjustments to the CIS system. Can you make adjustments other than changing the seasonal ---

A. (Lanteigne) Yeah, and thank you for that question. Just so I can clarify, you know, a

change to the actual estimation program in CIS would require programming that, again, as we've talked about, I think is not possible. From our perspective, the ability to determine and inform CIS of what period to use warm versus cold, that would be the minor adjustment. It's not a change to the programming logic. Thank you for clarifying that.

Q. That's fine. And on the last point, but the concern is that if you start doing changes to the programming, if I understand you correctly, you may lose the ability to issue bills on time and accurately to the vast majority of the people that are receiving bills. Is that a concern?

A. (Lanteigne) If the Customer Information System was not available for some reason, we could lose the ability to issue bills for all customers, yes.

Q. Okay. At the risk of having Mr. Clarke indicate that the question has been asked and

answered and Mr. Williams saying that it's not relevant, I'm going to go into the issue of the commitment that Nova Scotia Power made with respect to the costs associated with the restoration of the system. And I'm not going to go into any detail. I'm looking at a high level. I'm not even going to point to the actual specific costs.

But if I understand correctly what the commitment is, there was, in 2025, costs incurred that are being tracked, but rates did not increase in 2025, so those costs, by definition, can't be included -- can't increase the rates because the rates were already approved in 2022. Is that basically for the 2025 costs situation?

A. (Williams) Yes. Just to maybe say it in my own words, the rates for 2025 would have been approved in 2022. Actually, I think maybe the decision was early 2023, to be exact. But in any event, they would have been approved as part of that GRA sub rates for '23 and '24. Rates were not adjusted, as you've indicated, in '25, so the costs that would be in customer rates would

have been as forecast when the application was filed in 2022.

Q. And for the 2026-'27 period, any known cyber costs that relate to restoration were not included in the projected forecast; is that correct?

A. (Williams) That's exactly correct. It's the same premise or principle, but just the timing is obviously a little bit different in that the forecast for the '26-'27 General Rate Application was completed and put into application form prior to the event happening. And so again, there were no costs related to the cyberattack included in the forecast revenue requirement that was approved as part of the '26-'27 General Rate Application, which then means, as you've indicated, that there are no costs associated with it in '26 or '27 rates that customers will pay.

Q. Right. And really the only way that you could include, say, operating costs or any costs that are associated with the restoration process under

general principles would be to do an application, like has been done in the past for extraordinary remedies to include that cost that's not included in rates already?

A. (Williams) To include any costs that were incurred in '25, '26, or '27 in customer rates, there would need to be a deferral mechanism approved that would carry those costs forward for recovery in a future period.

To the point of the discussion yesterday when we talked about capital costs, if there's any costs associated with capital projects that are related to a delay, was the example yesterday, stemming from the cyber incident, to the extent that, again, there was a delay, there was costs associated with that delay and that those costs have been deemed imprudent, those costs on a forward basis would not be included in rate base as approved by the Board in whatever capital application we're talking about.

Q. I think the point that Ms.

Rudderham was making about that and the fact that the -- this situation, and I don’t know if this is -- in theory, if the project is put forward in 2026 while this process -- and this process alone is not looking at the entire picture of the cyber incident, the causes and so forth -- it doesn’t look into causes at all to some extent from a technical point of view. A project before the Board in that timeframe, before this proceeding and the technical proceeding is completed, a project before the Board is not going to address whether there’s been prudence or imprudence in relation to the cyber incident because it’s not completed. I think that was part of the conundrum that Ms. Rudderham was trying to point out. What do you say to that?

A. (Williams) Well, I think -- and again, it’s the same discussion that I had with Ms. Rudderham. I don't think we need to reinvent the wheel, if you will. The processes that exist in places, whether it's a capital application or the discussion we

had about the FAM, are certainly available and able to address those issues.

So to the extent that there's any costs in a capital -- to use your example, if we were to come forward with a capital application in '26, or at anytime before there's been an opportunity to fully assess the cyberattack, if there are costs associated with a delay, and those costs relate to the cyberattack, then I would envision the Board has the ability to identify those costs and make any decision that it had to make in relation to that capital application, contingent on an ultimate determination on those costs.

[9:50:15] **Q.** Okay, thank you.

Just a short one. In the evidence, it talks about the company not being aware of any customer-reported fraud or identity theft that's been reported to the company; that was when the IR responses were filed. But I'm just wondering as of today's date, do you have any information about any company customer-related fraud or

identity theft?

A. (Lanteigne) As of today, the panel is now aware of any reported.

Q. Okay. I'm going to talk about phishing, and I'm going to go to a different exhibit than what was discussed yesterday. In fact, part of that exhibit I think had some of the answers to the -- some of the information that was asked in the undertaking.

MEMBER MELANSON: But it's Exhibit N-11, at PDF page 19. N-11, at PDF page 19.

And just scroll down a little further, at line 16, but I'm going to look at that whole chart. Thanks.

BY MEMBER MELANSON:

Q. So this actually has the information from -- for the phishing results, test results from April of 2023 to April of 2026. The one -- because we've already discussed some of these, the 17 percent and so forth, in February of 2024. But the one that was sort

of standing out to me is the 14.3, sorry, not 14.3; 9.6 percent in September of 2025. So can you just look at -- sorry. September of 2025. Yes, 9.6 in September 2025.

And this is, you know, just a few months after the cyber incident, and I'm just wondering if that particular failure rate would have been a bit concerning to the company.

A. (Lanteigne) Maybe I'll start and Mr. Willams might add. I think from our perspective, to elaborate on what we talked about yesterday, you know, Nova Scotia Power takes these phishing exercises and failures to phishing very seriously. So the 9.6 percent failure in September of 2025, that you highlight, that would have been something that we would have talked about at the senior level.

Mr. Williams, I think yesterday mentioned that at Director and up levels there would have been discussions happening. There would have been also -- anyone who failed these exercises, as well, would have

been notification to the senior leadership of the departments, including the executives are aware of failures.

Employee follow-up would include follow-up from their direct leader. It would also include being registered in remedial training to go and actually learn more about the error that they specifically committed.

And as well, as we talked about, you know, additions that were made to the follow-up of consequences for employees who are not acting on the phishing exercises. That there is actually potential financial repercussions for employees moving forward if they have multiple failures in the run of a year.

I think, again, just one piece we talked about yesterday that I think is really important about these tests is they are designed to be very difficult. And we -- while we don't like to see the failure rates increase, we are actually -- it's a good

thing. That the training is -- and the exercises are very difficult because we want to make sure that we can prepare as best as possible for phishing attacks against Nova Scotia Power.

And Mr. ---

Q. On the ---

A. (Lanteigne) Sorry.

Mr. Williams, anything to addition to that? Okay.

Sorry.

Q. On the training aspect, I'm assuming that there is regular training, we've already talked about this. So there's not training before every test.

A. (Lanteigne) Not exactly, but Nova Scotia Power does actually conduct quarterly training with all employees. It's just mandatory for all employees to complete quarterly training. The additional training, that would be targeted to employees if they actually fail.

And interestingly enough, Mr. Williams talked yesterday kind of about the cultural changes that we've seen at Nova Scotia Power with regards to keeping an eye out for potential phishing attacks against the organization. And employees who do pass, as well, you know, there's that immediate validation of the pass.

So when you report the phish through the email systems that we have, you get instant confirmation that you have successfully passed the phishing test. So even if you're not doing the training because you failed, you're getting the validation that, and the reinforcement, that yeah, you did the right thing. You caught it and you successfully passed this exercise.

Q. There's one aspect, actually talking about remediation and steps taken after the results are known. And I'm just going to go to the rebuttal evidence at page, sorry, at N-17, PDF page 22, and at lines 22 to 27.

And this is in response to

recommendations about restricting computer access for failures into the policy standards. And the response is, "Regarding computer" -- or the rebuttal says:

> Regarding computer system access controls, NS Power must balance risk with ensuring employees have the tools they need to perform their job function. Further, access to NS Power's computer systems and data are granted, limited, and maintained based on the requirements of each role.

And it says:

> To [Nova Scotia] Power's knowledge, restricting computer system access is not currently a common disciplinary or punitive practice.

And my question is, if computer access is restricted to what the current employees need to fulfill their roles, currently, if you restrict it further, doesn't mean that they wouldn't be able to do their role at all?

A. (Williams) That's exactly right. So if we're in a situation where someone is a risk in that they are continually failing phishing tests, to the point

where we would need to restrict their access and limit the ability to do their job, we're not having a discussion about limiting access on the computer; we're having a discussion about continuing to work.

Q. So it's a dismissal type of issue ---

A. (Williams) Yes.

Q. --- as opposed to a training issue.

A. (Williams) Correct.

Q. Just some short questions.

MEMBER MELANSON: It's -- the next one is at Exhibit N-2, PDF page 6. N-2, PDF page 6, lines 18 to 20. And it's part of the discussion about the TransUnion protective features.

MR. NORWOOD: (Inaudible due to off microphone.)

MEMBER MELANSON: Yeah, no problem. I'll wait until it's up there. Just setting the context.

MR. NORWOOD: Page? I'm sorry.

MEMBER MELANSON: Sorry. PDF page 6, lines 18 to 20.

BY MEMBER MELANSON:

Q. And it's the Dark Web Monitoring portion of it. It talks about Dark Web Monitoring being available, but:

> ...which monitors surface, social, deep, and dark websites for potentially exposed personal, identity and financial information and helps protect individuals against identity theft.

This is actually the information coming from TransUnion. I'm not sure if you have any familiarity with this, but my understanding is to access that service there is a proactive step when you register to be able to access that particular function. Is that correct?

A. (Lanteigne) You are correct, that was a TransUnion service. Based on my knowledge of the service, once you've registered for myTrueIdentity, you

can actually go into that section of myTrueIdentity, and you can activate dark web monitoring for what information you want monitored.

Q. But it won't -- it's not a monitoring scenario where it's automatically if you just register with myTrueIdentity you will automatically have that monitoring. You have to actively go in and request it?

A. (Lanteigne) That is correct. It's another step that you would take in TransUnion. What is automatic with TransUnion, though, is, is as you sign up, you know, the system is monitoring changes to your credit report, so if someone does -- if something happens to your report, you'll actually get notifications if there's been a change.

But the actual -- if you wanted to put a specific item to monitor on the dark web, you are right. That is a step that you would take in TransUnion software.

A. (Williams) Maybe, Mr. Melanson,

just to be clear, as someone who has gone through the process, it ---

Q. You're talking to someone who has as well.

A. (Williams) Well, just to -- for everyone else, perhaps.

It's not an onerous step. It's when you register, you're entering the relevant information you want monitored and then you're simply ticking a box as part of that registration. It's not like it's an additional substantive step. It's all part of the process.

[10:00:14] **Q.** When I tried to register, I was advised that the information I provided was wrong, it wasn't what they already had in their database. I wasn't aware I was already in their database through my bank, so it's one of those strange situations.

Anyway.

Just another short one. Exhibit N-2,

PDF page 7. And it's in the middle of the page somewhere there, but it talks about -- it's about communicating with clients and it's discussing -- there's a reference to a national search optimization. I didn't know what that was, what a national page search optimization is.

A. (Lanteigne) Essentially, what it would mean is if you're using search engines such as Google, the -- certain keywords would be -- essentially, Nova Scotia Power would ensure that our results come up first to help provide information.

I think when an incident like this occurs, you know, it's -- we know that customers will reach out to searches of information like the internet to search for info, so we tried to ensure that if someone was searching for, you know, "Nova Scotia cyber incident," for example, they would be able to find that detail that would be helpful.

And as we've talked in our various updates to this incident, we have provided information on

our website as well to help customers understand the incident but also how to sign up for myTrueIdentity and other steps that they can take to protect themselves. So we just made sure that, as customers were leveraging search engines, they were able to find information that would help them in this regard.

A. (Williams) Mr. Melanson, I'll just add one of the reasons that, you know, page search optimization is as important as it is is not just what Mr. Lanteigne identified, which is that it pushes it to the top of your search results and makes it apparent and obvious, but when incidents like this happen, it's -- the potential also exists for websites to be spoofed, and so if someone were to search "Nova Scotia Power" and there's a spoof website out there, we took this step to ensure that our actual web page was the top and not some spoofed page.

So there's that added reason, not just the availability of the information, but the security of

the information that they're receiving as well.

Q. Okay.

MEMBER MELANSON: Those are my questions, Mr. Chair.

THE CHAIR: Mr. Deveau?

VICE CHAIR DEVEAU: Rob, could you pull up Board IRs Exhibit N-2, PDF page 23?

QUESTIONS FROM VICE CHAIR DEVEAU

Q. So panel, just continuing on some questions Mr. Mahody asked you late yesterday afternoon about the two letters that went out notifying customers May 10th and in relation to the Social Insurance Number, so what you see on your screen here is Exhibit N-2, IR-1, Attachment 2.

So that's the second letter which contains the reference to Social Insurance Number. The prior -- the other letter essentially identical, if you agree, except -- but for the reference to Social Insurance Number at the end of that sentence?

A. (Williams) Yes, sir. And that would be Attachment 1, the other letter without the Social Insurance Number reference.

Q. Right. Right.

So Mr. Mahody referred to confusion over the two letters and -- by customers, and it was just -- the two letters were leading to, you know -- from what

the Board saw in the letters, there was like a comparison of both letters and, you know, why does yours have Social Insurance Number and mine doesn't. The use of the word "May" was there, which perhaps led to more confusion.

I'm just wondering if it would have been clearer for the public if you had taken out -- at the end of that sentence, if you had ended the sentence after driver's licence number and then just put in a new sentence saying, "Our records show that your Social Insurance Number was also part of the data that Nova Scotia Power had on our systems and they have been accessed by the threat actor."

Wouldn't that have been clearer, perhaps avoided some confusion?

A. (Williams) Wordsmithing on the fly, sir. It's an alternate way of putting it, and it may have addressed the confusion that has been raised by some customers.

I think it's important to kind of

contextualize it, and Ms. Valdetero does this in her evidence where, when you're communicating to a large amount of people -- and I say this not to diminish the concerns or confusion that arose with certain customers because that is -- that is acknowledged and that is understood. But there were a large number of customers that received this and didn't -- were not confused by it and understood it, didn't raise the concerns, at the very least.

I go back to the discussion I had with Mr. Mahody that we're talking about two things here. One is could we have been more precise with the information that we were identifying for customers that we had that was pertaining to them.

That is not something that would have been reasonably possible ---

Q. Yeah, I'm not talking about that.

A. (Williams) Yeah. No, I understand.

Q. I realize -- I understand what you're saying about the "May have been accessed."

A. (Williams) And so ---

Q. It's just the fact that there were -- there was a subset of customers that you had their Social Insurance Number on record, and that may have been accessed.

All I'm saying is, wouldn't it have been clearer if that had been specifically taken out of that first sentence and added another sentence so people knew -- there was no confusion, you know, my -- you know, one letter says, "Our records show that your Social Insurance Number was part of our records and may have been accessed"? Wouldn't that have been clearer?

And you -- yeah.

A. (Williams) So I think -- again, the two letters were done intentionally, one to identify the group that we had the Social Insurance Numbers for. Having this discussion today, could we have worded it

differently to address some of the concerns that were raised? Yes, I mean, I think absolutely.

Q. Suppose ---

A. (Williams) When you know the concern with the letter, you can address the concern, but in real time when we're drafting the letter and putting it out there, we don't know of that concern and that potential confusion ahead of time.

But yes, absolutely now, in hindsight with the knowledge of what the concern was, we could have drafted it differently to address that concern.

Q. I suppose my concern is exactly that.

The addition of those -- you know, those four words "And Social Insurance Number" was intentional. You obviously directed your mind -- whoever drafted this letter -- and I'm sure it wasn't drafted in five minutes. I'm sure a lot of people looked at this letter in terms of, you know, what's contained in this

letter. And you know, intentionally just adding that at the end of the list, I'm just -- again, you've mentioned in your Opening Statement and your rebuttal about transparency, and I'm just -- it was -- well, you've seen the letters and there has been a lot of discussion on this issue.

There's a lot of -- a lot of discussion was about the Social Insurance Number, and I think you realized that that was an issue when you intentionally added those words at the end, so...

A. (Williams) Yes.

Q. Yeah.

A. (Williams) So I -- two points I'll raise, and one was what I'd discussed with Mr. Mahody, that the "May" at the start of this is intentional to make sure it's clear that we don't know definitely ---

Q. I understand.

A. (Williams) --- what was -- what was access.

Q. I understand that, yeah.

A. (Williams) The other is, I think -- you know, I understand your point and, as I said, in hindsight I can get there.

These letters were drafted with advice from external experts who would have advised on a number of different responses, and they would have had input on the wording of these letters as well. And so to a certain extent we were relying on their experience and what would have been appropriate and reasonable in response to past breaches, but I certainly appreciate your point that now knowing what the concerns we could have been different, we could have provided a different language.

Q. Yeah, okay. And just to follow a point there, my understanding was that customers could call and find out what you had in your CIS system; correct, about them?

[10:09:57] **A.** (Lanteigne) That is correct. And I think to add to what Mr. Wiliams indicated, recognizing

that the data that was affected was different than what was the current information in the Customer Information System that did contribute to some of the ---

Q. That was my question.

A. (Lanteigne) Yeah.

Q. So if a customer called to ask if you had that on your records, their Social Insurance Number, the answer -- on our Customer Information System, your Social Insurance Number is not contained in that system, but it had been purged by then, obviously; correct?

A. (Williams) So, yes, it brings me to another point that we should have discussed perhaps earlier. So we would have at one time had their Social Insurance Number.

Q. Correct.

A. (Williams) It would have been purged -- but it also could have been purged prior to 2024 and prior to 2021, so you know we may have had your Social

Insurance Number at one point in time. It doesn't necessarily mean that it was part of the cut that went into the Data Lake. Are you following me, sir? Because we did purge some Social Insurance Numbers between 2018 and 2021, so ---

Q. Right. But when a customer called you could indicate whether right now you have -- customer calls, "Is my Social Insurance Number on your system?" Then you could say no, but were they also advised that, "However, it may have been included in the information that was accessed"?

A. (Lanteigne) You are correct. There's very specific, you know, scripting that we did provide to our customers service associates, and really the important point was for customers to follow the guidance that had been provided in the letter and take the steps provided in the letter and protect that information because we didn't -- to avoid -- the discussion has been we did not -- we don't have on the current system what was

necessarily affected, so...

Q. So in the incident report it mentions the -- it has the questions that TransUnion had access to. I may have missed it, but I don't recall seeing -- I don't recall seeing that particular script that it's not on our system now, but it may have been accessed; is that one of the questions and answers?

A. (Lanteigne) TransUnion would not have had access to our Customer Information System so they would have not answered that question.

Q. Okay. So if it was escalated, it would come to you?

A. (Lanteigne) Or if a customer called us directly.

Q. Right, okay. Did you have a script for that?

A. (Lanteigne) Yeah, essentially it's what I talked about. It's really just, you know, "Yes, we can confirm what's on file but protect yourself

based on what you received in your letter.:

Q. Okay. I didn't realize that. So they would have access to the TransUnion list of questions that were contained in the incident report, but they had a separate bunch of -- series of questions and answers as well?

A. (Lanteigne) Our customer service associates had a lot of the same questions that the TransUnion general question line would have had but we would have had the ability to answer questions about, like, regular service (inaudible due to mumbling) on our current system, yes.

Q. But in terms of the -- about the cyber incident, there was a separate script for Nova Scotia Power staff to answer those questions about the cyber incident?

A. (Lanteigne) Yeah, essentially just to take -- to address situations like the one we're talking about; like, what is currently on the system.

Q. Right.

A. (Lanteigne) Just to answer questions like that because, again, back to this conversation about the letter, we do understand that the data that was affected and the current data on the system were not necessarily the same, so we just wanted to make sure that, you know, yes, we can answer questions about what we have on the system, but also make sure that customers are aware it's important to take the steps to protect themselves as outlined in the letter.

Q. Right. So did you have an actual script as you did for TransUnion? Is this something you can provide?

A. (Lanteigne) We could take that as an undertaking, yes.

Q. Okay.

VICE CHAIR DEVEAU: Can I ask for that, Chair?

BY VICE CHAIR DEVEAU:

Q. So again, I'm not asking you to prepare anything, but you had a script for ---

A. (Lanteigne) Yeah. Yeah absolutely. No, no, it's a fair question and I appreciate clarifying kind of the different experience between the two groups. Thank you.

THE CHAIR: Undertaking U-12.

UNDERTAKING U-12 - To provide the script given to Nova Scotia Power staff to answer questions about the cyber incident

VICE CHAIR DEVEAU: The compliance letter from the Office of the Privacy Commissioner of Canada; I think it's on the record as part of, Rob, N-11 which are the Small Business Advocate IRs. So it would be IR-18, and it would be -- Rob, it would be N-11, PDF page 32, and then can you click -- are you able to click on there? Will that work for you to click on there and bring that up? Yeah.

BY VICE CHAIR DEVEAU:

Q. So in terms of the compliance letter, that is -- both terms were agreed to between the Office and Nova Scotia Power, I assume; that there was some discussion about the contents of that letter before it was published? It was consensual of what went up in terms of what was issued?

A. (Williams) To the extent that say there was discussion, it was not an negotiation.

Q. No, no, no, I realize that.

A. (Williams) There was discussion obviously. It was offered to us as something that could be signed and agreed to.

Q. Right. And you agreed to it?

A. (Williams) Yes. Yes, it was signed.

Q. Now, just one issue that I saw in it, and I'm just wondering in terms of the Statement of Facts.

VICE CHAIR DEVEAU: If we go to -- just a little bit down, three or four headings down, Rob, it starts, "Complaints received by the OPC"; it's a heading. The next one. Yeah, right there.

BY VICE CHAIR DEVEAU:

Q. So under, "Complaints received by the OPC," the second bullet there. It says one of these complaints related to the collection and retention of SIN numbers. And then it says:

> Nova Scotia Power explained that SINs were included in the data accessed and exfiltrated by the threat actor from a data repository related to the organization's program for the provision of energy usage insights to its customers. (As read)

So if we keep that in mind, and I'd refer you to the rebuttal N-17, page 30. And it's at line 5. It says, "The Attack involved unauthorized access to data stored on NS Power's NAS..." which is a network attached storage, "...and within its Azure Data Lake environment, which contained tens of thousands of files."

And it's also referred to again at page 55.

VICE CHAIR DEVEAU: If we can go to page 55, at line 14. Yeah, so just show -- show me the whole paragraph there.

BY VICE CHAIR DEVEAU:

Q. So it says:

> As part of that conversion effort, individual employees migrating data from the NAS to SharePoint Online...

And that was relating to another function, not the Energy Insights:

> ...that data would be cleansed from data migrating to SharePoint Online. While this work was scheduled to occur, the Attack preceded the work being undertaken. As a result, personal information (retained longer than the timeframe set out in the retention schedule) existed in the NAS at the time of the Attack and some of the drives containing this information were accessed by the threat actor.

So that seems to be another source of data that was accessed during the incident. And I'm just wondering why that would not have -- was the Office of the Privacy

Commissioner aware of that additional infiltration?

A. (Williams) Yes, sir, my understanding would be that they were certainly aware. This section that we're referring to is specific to the -- they're summarizing the complaints they received and they're talking about the summaries in particular.

Q. So it's not something that came after the complaints letter or anything?

A. (Williams) No, sir.

Q. They were aware about that too?

A. (Williams) Yes.

Q. Okay.

VICE CHAIR DEVEAU: Rob, can we go to Nova Scotia Power's Opening Statement, N-21?

MR. NORWOOD: Exhibit N-21?

[10:20:49] **VICE CHAIR DEVEAU:** Yeah. And it's the first paragraph we're looking at, page 1, first paragraph.

BY VICE CHAIR DEVEAU:

Q. You say at the end of that paragraph:

> We acknowledge the work ahead of us to improve our customers' trust and we are committed to earning it through transparency and accountability, including being here today to discuss the Attack and our response in more detail.

VICE CHAIR DEVEAU: And then at the penultimate paragraph at the bottom of the -- I think it's at the bottom of the page -- sorry, it's at the very end, the very end of the document, the second-last paragraph there -- sorry, go back to that first page. It's the penultimate paragraph, but I must have meant the penultimate paragraph on that page. Right there. Yeah, it is. Sorry, it was the penultimate paragraph of that first page.

BY VICE CHAIR DEVEAU:

Q. The last sentence there:

> We accept accountability for the stewardship of the customer information in our care, and we accept responsibility for continuously strengthening our safeguards against evolving threats.

My question is just a general question. Could you describe how the Company has accepted accountability for the customer information in its care? I'm just wondering what do you mean by accountability? Is it more than just essentially committing to not charging customers for restoration costs? Is there -- what does accountability mean?

A. (MacDonald) Thank you for the question, Mr. Deveau. I think really what's intended there is in the totality of all that we've acknowledged and are attempting to be as transparent and accountable as possible about, whether that be explaining how the billing has worked, explaining the commitments in the privacy letter -- the Office of the Privacy Commissioner letter, that is -- that's what we're getting at there is just a general totality of what has happened and how we are going about it is the accountability there.

Mr. Williams might want to elaborate

on anything sort of specific or from his point of view in terms of what we mean by those words.

A. (Williams) I certainly agree with what Ms. MacDonald has said, sir. There's no one aspect to this that I can point to that's demonstrating our accountability. It's the aggregation of everything, and so the commitment you referred to, the commitment letter that we were just talking about with the OPC, going through and undertaking that process with the OPC and not just going through that process. It's not a choice to go through that process, but the manner in which we go through that process matters, just as it does this process today and the process that will follow this one. It's not just about participating in those processes but the manner in which we do so, the manner in which we show up, the manner in which we're providing evidence, attempting to be as responsive and transparent as we possibly could be, and part of that is also acknowledging where we have work to do or enhancements to make or what we need to do in the

future to ensure that something like this does not happen again, to the best of our ability.

So to me, it's the totality of that and it's not just, you know, tangible things that we can point to, but it's also, as I said, the approach we take and the commitments we make along the way. You know, Ms. MacDonald said in the Opening Statement that it's actions, it's not words. So while it's, I'm sure, some comfort to hear us speak today and hear myself and Ms. MacDonald say these words, we know that there's work to be done to demonstrate that accountability is something that we take seriously and something that we've accepted.

Q. I ask this on behalf of customers because you've read the letters of comment, and for many customers, accountability means repercussions. And I'm just wondering in terms of those types of questions, what would be your response to that?

A. (Williams) So I certainly understand that the perspective of some may be that

accountability means repercussions. I wouldn't necessarily agree with that, but I certainly think it does mean that there must be actions taken, regardless of whether those are repercussions or not. I think it's important to understand that, and as we've discussed and as is included in CA IR-6, there are significant costs that the Company has already incurred as a result of this that customers will not pay for, and we discussed those, and I'm happy to do so again, but I think everyone is aware. We've also talked about in addition to those costs, the cost of carrying -- the carrying costs for the customers' outstanding bills, the lost revenue from late fees. So there's a number of different avenues where there has been a financial -- a significant financial impact to the Company already.

So if we want to talk about repercussions, those are financial repercussions that are very real and very significant for the Company and its shareholder.

In terms of actions, which I think is perhaps the more constructive approach to this discussion, we, I think, have identified a number of different actions that we're taking thus far. Already in this proceeding there's a number that are outlined in our rebuttal evidence of constructive things, tangible things that we are doing, again, to enhance our stance both from a privacy perspective but also from a cybersecurity perspective, and you'll hear much more about that in the compendium process.

So, you know, accountability is a number of different things. In terms of actions going forward, there are, I think, a plethora of evidence that we take that very seriously, that we've identified a number of concrete actions on a go-forward basis, and there will be more to come as we move through the audit process with LevelBlue, and you'll be seeing the outcome of that. I full expect there to be more work to be done and more deliverables that we'll add to that list of the

actions that we'll take forward.

Q. Okay. Let's get into some of the matters. The first, I'd like to refer you to the incident report.

VICE CHAIR DEVEAU: Rob, that's N-16, and it's about the removal of Social Insurance Numbers. So let's go -- it's N-16 and it's the section on page -- I think it would be page 43. Yeah.

BY VICE CHAIR DEVEAU:

Q. So this is where you go through the history, starting at line 16 there. In 2018, you -- there was a practice to collect the Social Insurance Numbers and in 2018 you changed that practice to no longer collecting them. And then in May of 2024, line 23:

> In May of 2024, NS Power developed and commenced a process to purge customer SINs from the CIS environment.

So we've reviewed that already. Then the next page, at line 16, you say:

> On June 25, 2025, Nova Scotia Power publicly committed to permanently deleting instances

of SINs that remained in the Company's system.

This, of course, was after the breach and when you committed to deleting the rest of the SINs.

It said:

The Company has initiated a process to identify and remove instances of SINs contained within its records. It later confirmed this was substantially completed by March 31, 2026.

I realize there was some more that were found, but I'm just -- generally where I'm at in terms of this question is where you were at the end of March.

So when you say -- it says here, "The Company initiated a process"; I'm just wondering, was that a different process than the process that had been used in May of 2024 to purge the other -- you know, to generally do the purge that you thought had caught most of these? Is that a different process or were they -- yeah.

What was the difference between the

two processes?

[10:30:45] **A.** (Williams) Yes, it would have been in -- so it was external or third-party confirmation of the deletions, so that would -- that was -- that, in of itself, was different than what was done in 2024.

So 2024 was done internally. This was identifying external parties -- or party or parties that could undertake the work and provide the confirmation that it had been removed. And it was also a more robust process where it was scanning all systems within the company to ensure that we could make the statement that they had been permanently removed from all systems within the company.

Q. Okay. So that was my question.

Why -- in 2024, why was the purge -- was the purge isolated to the CIS system? Why, at that point, didn't -- wasn't the question asked, okay, where do we have Social Insurance Numbers on all our systems? Why wasn't it done in 2024?

A. (Williams) It's a good question, sir.

And so at the time, in 2024, the understanding would have been that the Social Insurance Numbers resided within CIS. And as we discussed with the Data Lake, those Social Insurance Numbers were there, but there was a process -- an automated process to remove them. There would not have been an expectation that there would have been Social Insurance Numbers elsewhere.

Having now gone through this attack and the restoration process and understanding that there was the potential for unintended -- for Social Insurance Numbers to be in places on our systems in unintended manner, we thought it prudent to search the entirety of our systems as opposed to the CIS where they reside.

Q. There was an undertaking yesterday about -- the Chair had asked for the undertaking what the 13 terabytes that was accessed -- what percentage of that -- was that of your total IT network.

I'd like another undertaking, and that would be the volume of the data in the July 2021 cut in the Azure staging area. What was the volume of that data in that July 2021 cut? Is that -- in terms of the actual size. Is that something we can -- we can get as an undertaking?

A. (Williams) I'm generally getting nods, sir, so I'm going to say yes. And we'll certainly let you know if that's ---

Q. Okay.

A. (Williams) --- it's not possible. But my understanding is that it is.

Q. Thank you.

THE CHAIR: That will be Undertaking U-13.

UNDERTAKING U-13 - To provide the volume of data in the July 2021 cut in the Azure staging area

BY VICE CHAIR DEVEAU:

Q. So just -- again, just to the -- to the process that we just described of what happened in 2018 and then 2024 -- so after the breach in 2025, essentially you purged the remaining Social Insurance Numbers within a year, probably within nine months or something to that degree.

I suppose it begs the question, where was the urgency between 2018 and 2024, recognizing that you shouldn't be retaining -- in 2018, you recognized that -- the company recognized that you shouldn't be retaining SIN numbers, so I'm just -- I'm just wondering -- you were able to do in 2025 within nine months. Where was that urgency between 2018 and 2024?

A. (Williams) Yes. And again, sir, fair question.

I think the ability to do it quicker in 2025 was in part because we'd already gone through the exercise and we already knew what was possible within the CIS.

Q. So that's in terms of technical issues?

A. (Williams) So the technical issues, the risks that are posed by doing that type of work within the CIS. So we had already completed that work and so didn't need to revisit the discussion of weighing those risks and benefits.

Q. Rebuttal N-17. N-17 at pages 60 and 61.

So this relates to actions that you took to enhance your governance program.

So essentially, in those -- in that -- in those few paragraphs, you explain the steps taken by Nova Scotia Power to enhance your governance program. You outline the revised role for the Privacy Officer and the reporting structure through the Executive Vice President Finance and Commercial, the Executive Leadership Team and to the Board of Directors as -- bringing it up as a standing agenda item.

I could let you review that, but it's pretty straightforward, yeah.

So I'm just wondering -- I have a number of questions about that. I'm just wondering, why is that description in the rebuttal? What evidence -- what evidence are you trying to rebut there? I wasn't quite sure why it was in the rebuttal and, actually, why the information wasn't provided in the incident report.

A. (Williams) No, and it's -- it's maybe more of a process question than anything, sir, I think.

So I mean, we've called this rebuttal and I think it was termed "rebuttal" in the process schedule, but it's our first instance to put anything on the record in this proceeding.

So the incident report, as you'll recall, was something that was filed in 12273.

Q. Right.

A. (Williams) So I -- so in

fairness, it wasn't put in there just because there wasn't recognition of what the scope or the focus would be. That has obviously evolved with the introduction of 12600 ---

Q. Yeah.

A. (Williams) --- and the issues list there.

Q. Okay. I understand that. That's fair.

A. (Williams) So I don't see it necessarily as rebuttal, but it's ---

Q. I understand.

A. (Williams) --- to (inaudible due to speaking over each other).

Q. Understand. Okay.

So when were those steps actually -- those -- that new reporting structure, when were those steps actually sort of implemented, generally?

A. (Williams) You're referring to the first three bullets?

Q. Yeah, yeah.

A. (Williams) So those are -- those are ongoing, so we will have -- we have -- well, they're current, I suppose.

We have a posting. We are currently searching for that Privacy Officer position.

That is, again, not to say we don't have and have not had a Privacy Officer. We do have one. But we are looking to fill that position currently, and the exact timing of that will be dependent on the market response.

Q. Okay. So at the bottom of page 60 there, it talks about the Privacy Officer and the enhanced role, and perhaps -- I'm not sure if it's -- yeah, more enhanced and formalized, dedicated full-time position.

It says at the bottom -- at the bottom sentence there:

> The internal reporting structure for the

> Privacy Officer will be determined based on seniority level of the successful candidate but is anticipated to ultimately report up to the Executive Vice President Finance and Commercial...

And first of all, just so I -- I understand now that the Privacy Officer at present is not a full-time position; is that correct? That basically the role is assigned to a lawyer on the legal team somewhere in the organization, and it's part of other duties that person provides?

A. (Williams) Yes, it's currently the Director of Legal within Nova Scotia Power.

Q. Okay. And you say there that:

> The internal reporting structure for the Privacy Officer will be determined based on seniority level of the successful candidate...

With all due respect, I find that's an odd statement. I would have thought that if the role is being enhanced, but you're saying that the reporting structure will depend on the seniority of the candidate, so the reports will change depending on that seniority. I

would have thought that the seniority and the duties of the position itself would inform reporting structure. [10:40:03] I'm just wondering if you're -- if these changes are actually empowering the Privacy Officer with the sufficient authority and responsibility to be effective in their role, rather than just depending -- putting them in the organization based on where their seniority is. I would have thought seniority would have been decided.

A. (Williams) So two parts to that, I suppose. The mandate and authority of the Privacy Officer will not differ. That Privacy Officer will report up through myself, to the Executive Vice President of Finance, and that mandate will be the same regardless, I can assure you of that.

The seniority, though, will be dictated by the market response. And so all this sentence is indicating is, you know, whether that is a lawyer who is a 5-year or a 15-year call, where they sit within the

reporting structure may differ.

And it would not be -- it may be that if we have, and this is a bit of a marketing pitch, if we get a unicorn that has 15 to 20 years of experience as an ex-Privacy Officer at a large company, that's going to change how we establish that structure. And they maybe don't report up through me after if that's the case, right?

So it's a -- it's just acknowledging that while the intention to prioritize this, exactly what that reporting structure will be and the governance of it, is going to be dependent on that candidate's experience.

Q. Do you have evidence that those type of people are tough to find?

A. (Williams) Well, if you go ---

Q. Along with engineers and other positions.

A. If you -- yeah. If you've gone to market for any legal positions recently ---

Q. Legal positions in privacy you mean, or...?

A. (Williams) Well, I'm just talking generally.

Q. Okay.

A. (Williams) It's difficult to find specific skillsets. So -- and by that, I mean, you know, whether it's privacy or anything else. That specific skillset is in demand. I am confident we will find an appropriate Privacy Officer, though.

Q. Okay. So there's a recognition that, regardless of the seniority of the position, that the duties that are performed by the Privacy Officer will be given the respect it deserves as to the organization. I mean, that's an obvious question based on what's happened in the last year.

A. (Williams) Yes, the question and answers. I don't want it to come across, though, that the Privacy Officer did not have the respect it deserved prior

to the incident because it ---

Q. Yeah, and I ---

A. (Williams) --- it absolutely ---

Q. I didn't mean it that way. Just mean ---

A. (Williams) No, I ---

Q. --- in terms of if you're revamping the reporting structure, it just seemed -- yeah.

A. (Williams) Even absent this event, sir, and what we've experienced the last year, there's significant change afoot in the privacy environment within Canada.

Q. On page 61, I think it's in the second bullet there, it says:

> The [Executive VP] Finance and Commercial will brief the [Nova Scotia] Power Board of Directors on privacy related matters as a standing agenda item on a quarterly basis.

So at the time of the incident, then, did anyone report to the Board of Directors regularly, or otherwise, on privacy matters? Was it a -- an issue that

was brought by way of practice to the Board?

A. (Williams) Yes, sir. So at the time of the incident, it would have been the EVP of Legal, Regulatory, and GR, and that reporting would have been done on an as-needed basis, as are, you know, a number of different matters.

Q. Okay.

A. (Williams) The intention here is to point out that the additional action that is being taken to make this a standing agenda item on the Board's quarterly meeting agenda ---

Q. Okay. So that's a new ---

A. (Williams) --- on a go-forward basis.

Q. That's a new practice.

A. (Williams) Making it a standing item, but the reporting function always existed.

Q. Okay. So now, my questions now are in relation to compliance. Not the policies

themselves, but compliance with the policies.

So at the time of the incident, what was process for ensuring compliance with the privacy and data collection and retention policies? Who made sure that the policies -- that what the policies said were -- was actually carried out? Again, in terms of compliance.

A. (Williams) So depending on the specific aspect of the policy or procedure, it would ultimately have been the responsibility of the Privacy Officer and the -- and management of the company to ensure that those -- the policy and the procedures that fall under it are being implemented.

Q. Okay. Was there a regular review of the policies in terms of compliance that are reviewed by the senior leadership team?

A. (Williams) So there was not a (inaudible due to audio glitch) of that, but there was -- there were ---

Q. You said there was not a recent

audit?

A. (Williams) Not, not a recent ---

Q. Yeah. Right.

A. (Williams) --- audit of the privacy program in totality. Obviously, there is aspects of it that, and we discussed one earlier, the Data Lake.

But there was -- as I said, the Privacy Officer would have oversight of certain aspects of it. There's also the Privacy Committee within Nova Scotia Power was interested with ensuring that the different business units were aware of their obligations under the privacy policy and procedures, as well as the training that was undertaken by our employees.

You'll see here, one of the bullet points does refer to the Privacy Committee. And I think one of the things we've taken from that, that Privacy Committee was established with members from different business units at -- effectively, at a manager level, being the job title.

And I think one of things we've taken away from this is -- and on a go-forward basis, is that we need to have that committee staffed with a higher level of responsibility within the company. So now that committee is staffed with Director level and above.

And I think the intention there is to ensure, and again this is the cultural discussion, to ensure that we have employees on that committee that are fully capable and have the ability to instill that culture, ensure that culture, and that the policies and procedures that are in place are being adhered within the different business centres.

Q. My understanding of corporate governance is that some boards actually have a compliance review on a regular basis. That -- let's say they have 50 policies that, you know, let's say 10 policies will be brought -- reported to the board every year, an evaluation done of whether there was compliance with those policies. Was that type of review ever done, to your knowledge, by

the Board of Directors on the cycle?

A. (Williams) Just referring with Ms. MacDonald, and neither of us are aware of that, that what you're describing there, but I think it's the other bullet point here, which refers to Optro. And it's the second from the bottom of the penultimate bullet point on 61. So that is a compliance program within Nova Scotia Power that's -- it's a manner in which we track compliance with certain obligations, whether they be legal obligations or internal.

Q. And sorry, that's the second ---

A. (Williams) The second bullet from the bottom on page 61, sir.

Q. Okay, "In the interim" -- okay. "In the interim," but that's a newly implemented compliance tool; correct?

A. (Williams) It's a new program; it's not a new compliance tool. That would be in brackets in the second line, beginning on line 23, "formerly known

as AuditBoard". So AuditBoard would have been in place at the time of the ---

Q. Of the incident?

A. (Williams) Yes. So just to be clear, the function existed, just the program and the name of it has changed.

[10:50:16] **Q.** Okay. I may come back to that.

So in terms of the Board -- I can bring it to you; it's discussed in NSPI's management information circular. The management information circular notes that Nova Scotia Power does not have the -- the Board does not have an Audit Committee and there are no other standing committees that would review compliance with these policies. Is that right, in terms of the Board of Directors?

A. (Williams) That's right. The Board does -- the Nova Scotia Power Board does not have subcommittees.

Q. Does not have an Audit Committee?

A. (Williams) Yes, it does not have any subcommittees.

Q. Right.

A. (Williams) Correct.

Q. Okay. And I'm sorry, in relation to the executive leadership team, was there a regular review of compliance with the policies? Again, compliance versus looking at the policies themselves and whether they have to be revised? I'm talking about compliance and what was said in the policies was actually being done. In addition to Optro, was there actually an issue that came to the executive leadership team and then further up to the Board of Directors about compliance?

A. (Williams) Sorry, sir, would you mind just repeating the question again?

Q. Was there a regular review by the executive leadership team to track compliance with the policies? So what I'm essentially going to ask is was it documented in terms of a schedule or listing of when these

compliance reviews about the policies would have happened and when -- whether that was documented?

A. (Williams) Not to my knowledge, sir, no.

Q. And then nothing would have been provided to the Board of Directors either from the executive leadership team?

A. (Williams) Again, not that I'm aware of. The reporting structure existed that if there were anything to report, it could have and would have been, but I'm not aware of it.

Q. Okay. So the results from Optro, who monitored those results? The internal compliance team, who's that? Is that that Audit Committee or Cyber Committee?

A. (Williams) So there's a Manager of Compliance within the legal group, within Nova Scotia Power, and they would administer the program. It is a function that's signed off by the relevant leader within

the business area. So again, this is not just -- as you'll see here, it's not just in relation to something like privacy. It's any and all compliance obligations that the company may have.

Q. CRA deductions and that sort of thing?

A. (Williams) So yes, sir, I can say it goes so far as to list any and all obligations that we have under the QA that I sign off on. So when I say any legal or internal obligation, it includes it.

Q. Yeah. So I had read that Optro as being an interim measure. So in terms of the former name, the AuditBoard, you've had that for seven, eight years, let's say?

A. (Williams) That's correct.

Q. Okay. And that's reviewed by the internal compliance team, or there's a report that's published?

A. (Williams) It's all automated, so

there's not necessarily a ---

Q. So there's a screen that says ---

A. (Williams) That's right.

Q. And the privacy policies are part of that screen? They're part of that?

A. (Williams) It would be in terms of whether they are confirming that the privacy policies are in compliance with whatever the development regulations or requirements are. In the interim language here is maybe a bit misleading in that it's in reference to the above paragraph or policies and procedures that ---

Q. Okay. So it talked about the policies but not compliance with the policies in terms of the policies are being implemented as they're supposed to?

A. (Williams) I can't confirm exactly what the wording is as I sit here, sir.

Q. Okay.

A. (Williams) But in effect, that is the audit -- that is the regular audit function within the

business, and in the interim is not that this is an interim measure; it's that it's anticipated that those policies and procedures will be updated as they relate to privacy, and that in the interim, the existing ones are being used.

Q. Okay. Thank you. I know we have to break, so I'll ---

THE CHAIR: Yeah, a bit of an extended break this morning. I apologize for that. So we'll come back at 11:30.

--- Upon recessing at 10:55 a.m.

--- Upon resuming at 11:30 a.m.

VICE CHAIR DEVEAU: Okay, I think we're reconvened.

GLEN MacLEOD, Resumed:

CHRIS LANTEIGNE, Resumed:

LIA MACDONALD, Resumed:

BLAKE WILLIAMS, Resumed:

VICE CHAIR DEVEAU: I'm just going to

ask Mr. Norwood to bring up -- it's the Retention Disposition Schedule; it's N-17(i), Attachment 2. Just a short question, just bring it up a little bit until we see all the audit. There's a second column. Yeah, right there. Yeah. Just expand it a bit. The second column where it says, "Audit," just make those a bit bigger.

In the second column "Audit" there, just bring that up. There's five of those columns -- there's five of those rows, I mean. Just bring the document up a bit. Right there. Sorry; one more. Right there, yeah, perfect.

QUESTIONS FROM VICE CHAIR DEVEAU, (Cont'd)

Q. It's just a minor question, but you'll see in the -- sorry; the row, "Audit, 001, internal audit document," there are -- it says, "Records in administrating compliance with internal policies and procedures" and it goes on. And then a couple of rows later, it says, "Audit 006". It says, "Internal Audit Document 6" and it has the same description in Column B.

So I'm just wondering, what's the difference between "Internal Audit Document" and "Internal Document Set"; what does that mean?

A. (Williams) Just give me one moment.

Q. Yeah, yeah.

A. (Williams) I think, Mr. Deveau, I'm happy to get an answer for you, but I'd have to take an undertaking just to confirm.

Q. It's probably very minor; I just want to know the references.

A. (Williams) I would expect it's an administrative difference.

Q. Yeah, okay.

VICE CHAIR DEVEAU: An undertaking, please?

THE CHAIR: Okay, that will be undertaking U-4 -- sorry; U-14.

UNDERTAKING U-14 - Re: Exhibit

N-17(i), Attachment 2, Retention Disposition Schedule, to advise what the difference is between "Internal Audit Document" and "Internal Audit Document Set"

BY VICE CHAIR DEVEAU:

Q. Yeah. So just for the transcript, it's the Retention Disposition Schedule, Exhibit N-17(i), Attachment 2, just to know the distinction between the two rows, "Internal Audit Document" and "Internal Audit Document Set." Just what the distinction is.

Okay. Getting back to that -- getting back to the discussion we had yesterday where you answered questions about transferring the data from the CIS system, to the staging area, to the MyEnergy Insights, let's go to the incident report which is, I think, I(10).

VICE CHAIR DEVEAU: Sorry; I think I've got the wrong number there actually. The incident

report should be N-16, sorry. And I'm sorry, I didn't get a page.

Sorry; can you search in there Rob, can you do a quick search for me, just search for the word "Encrypted," e-n-c-r-y-p-t-e-d. Sorry about that. That's the one. Okay. So it's at line 8. What's the page number on the bottom there?

MR. NORWOOD: Forty-four (44) of 46.

BY VICE CHAIR DEVEAU:

Q. Okay, 44 of 46. So right there it says -- so this talks about in 2021 when you initiated the MyEnergy Insights Program.

And in the fourth line it says:

> Within this staging area, certain daily exports from July 2021 were targeted by the threat actor for exfiltration.

And then you say:

> It is important to note that all data within the Azure environment was (and [still is]) encrypted at rest with only approved users having authorized access to that environment.

And I'm sorry, I'm missing the point that's being made here. Why is it important to note that? What's the point being made there?

A. (Williams) Yeah, no, it's a good question, sir. The point I think that's being made is to just make sure it's clear that this data wasn't just sitting there. And so when we talk about policies, procedures, and protections that are in place, ---

Q. Oh, I see.

A. (Williams) --- it's also the cybersecurity protections that are in place. So it was encrypted within that setting. It wasn't just sitting within the Data Lake. So the Data Lake itself is secure, but in addition to that encrypted within the Data Lake.

Q. Okay. Because it was still accessed but it was unauthorized, it was through the breach that it was accessed?

A. (Williams) That's right. And at rest just refers to the fact that it is sitting there and

not in transition between two systems that were the function of (inaudible due to speaking over each other).

Q. Okay. I understand, thank you.

My next question is, so the company realized in 2018 that it -- or it decided that it would not be collecting Social Insurance Numbers anymore. So I guess from a risk standpoint, why would the company risk further exposure of this personal information by expanding its storage and access to two other systems, the Azure system and the MyEnergy Insights Platform? Why would the company launch a new system like MyEnergy Insights if it did not have access to a clean, for lack of a better word, database that didn't contain inappropriate personal information?

(SHORT PAUSE)

MR. WILLIAMS: So I would say, sir, that is, in part, the purpose of the Data Lake, is to take data and cleanse it or purge it so it can move on to a purpose where the more narrowly scoped data is needed.

So it would have been understood that, from MyEnergy Insights, the data that was within CIS is not all required, but that would have been the point of moving it into the Data Lake and having the staging area, the production area and then on to MyEnergy Insights, so...

BY VICE CHAIR DEVEAU:

[11:39:56] **Q.** So once it's in the staging area, you only need -- if you only need certain part of that data to be used in MyEnergy, you might not need the, say, driver's licence if it's on there or an email address or ---

A. (Williams) That's right.

And so that's why when I referred earlier to the 14 and 90-day ---

Q. Right.

A. (Williams) --- construction timelines within there, the 14-day timeline would apply to data that had already been scrubbed or manipulated, so it

would move on and the assumption would be you've dealt within the 14 days.

Q. Okay.

A. (Williams) Any data that hasn't been touched would remain for 90 days with the assumption that we may still need it, we just haven't gotten to it yet. But after 90 days, it doesn't matter, you lose access to it. So ---

Q. So when the data's in the Data Lake, it can be manipulated more easily, and you take the information you need.

A. (Williams) That's right. It's a -- a work table.

Q. Yeah, yeah. Yeah.

And then you -- but then again, you are -- it's in your CIS system and you are exposing it to a risk. You know, it's another avenue that unauthorized access could gain -- an unauthorized user could gain access to it. It's -- it just feels like you're -- once

you're expanding it to other platforms or -- well, the SIN numbers probably wouldn't make it to MyEnergy, but when you're copying it from the CIS system to the Azure system, it's just another place where another unauthorized user could gain access.

I'm just wondering, why take that risk?

A. (Williams) So I think generally agree -- I would agree with you, sir, that -- the premise of the question. And again, this is not necessarily my area of expertise, but my understanding would be that it would be a general practice to take a dataset and then manipulate it, take what you need, and that's why the Data Lake was structured as it was. That's why Data Lakes are structured as they are, with the different phases and the retention periods that vary because it's understood that you're going to leave data elements behind. But I understand -- I certainly understand your point.

Q. And you were -- essentially, you

were -- the staff was relying on the fact that there were automated destruction tools in place that -- that would get rid of that.

A. (Williams) Yes, and you were doing it in a protected environment ---

Q. Right.

A. (Williams) --- as well, a secure, protected environment.

Yes, that would have been the premise.

Q. Yeah. And the Azure system is more -- yeah. Well, the comparison you made yesterday to the CIS system being a VCR, I took that personally because I do still own a VCR just in case, just for my favourite movies from the past, from the sixties and seventies.

A. (Williams) I'm sure my kids took it personally as well.

Q. But once it's in Azure, it's more easily manipulated by a cyber actor because the tools -- the tools will work more readily in the Azure environment

than it would in a vintage system.

A. (Williams) Now we are far removed from my ---

Q. Okay, that's fine.

A. (Williams) --- area of comfort, sir. Yes.

Q. Okay. Just a little question on training.

Training of your employees, one of the reasons to provide training to staff is ensure they are diligent about the cyber risks; correct?

A. (Williams) Yes, absolutely.

Q. Yeah. And cyber incidents like the one that occurred in this instance can represent a significant financial risk for the company. You'll acknowledge that.

A. (Williams) They have not just presented a risk, but they have made it a reality.

Q. Yeah. Correct.

So that was recognized in your financial statements, and Ms. Rudderham identified them yesterday. I was going to as well, but a different document.

VICE CHAIR DEVEAU: Rob, the email I sent you, could you pull out the one that's called the -- the one that's got highlighted on it. It's in Matter -- it's the 2025 Nova Scotia Power Annual Financial Statements, and it's Matter M12835, Exhibit N-2, Attachment 3. And it's the 2025 Management Discussion and Analysis.

And cybersecurity risk is identified in the document. Let's go to page -- it's PDF page -- sorry; page 21 of 30. It's -- yeah.

BY VICE CHAIR DEVEAU:

Q. So -- and just to show you the section on cybersecurity, it starts there and then goes to the next page.

VICE CHAIR DEVEAU: Rob, just show

them the entirety of the -- of that section.

Yeah. So it goes -- yeah. So it's four paragraphs total.

So let's go back to the first paragraph, and I'll just let you read that paragraph.

(SHORT PAUSE)

BY VICE CHAIR DEVEAU:

Q. So my question, it's about that highlighted sentence. So this was the 2025. This is the current, the ones that were just released.

I have it available, which I can pull up if you wish, and I have a redline as well. But the sentence that's highlighted there where it says:

> The Company increasingly relies on IT systems, networks and cloud infrastructure and third party providers to effectively manage and safely operate its assets...

Last year's version of this same section, practically all the wording is identical.

But the 2024 version, which would have been before the breach, it says -- where it says the

company increasingly relies on these various things, when it gets to third-party service providers to effectively manage and safely operate its assets, it -- last year's version included the word, "And the diligence of its team members" to effectively manage and safely operate its assets.

I'm just wondering, why would the reference to the diligence of its team members be removed from that sentence? Because I would have thought that is one of the elements that you rely on to manage and safely operate the assets.

A. (MacDonald) Thank you, Mr. Deveau.

I mean, I think the emphasis is shifting to reliance on expertise of third-party vendors in general, in particular in the areas noted here. That's not to say that we don't still implicitly rely on the expertise and diligence of our team members throughout the company, but the emphasis here is indicative of the shift

as we've described in other parts of this matter and the related matters, the shift towards vendor cloud-based expert service provision beyond what our internal teams would have been more focused on in the past.

Q. Okay. Will you agree -- it's not an insignificant deletion, though. Would you agree?

A. (MacDonald) I can't speak exactly to what was considered when this sentence was being worded.

Q. Pardon me?

A. (MacDonald) I can't speak exactly to what was being considered when the sentence was worded or reworded the first time or this time here.

Q. Okay.

A. (MacDonald) I take your point, but I wouldn't want to leave any overemphasis on this edit on the record here.

Q. Okay. I don't see it added -- well, it wasn't added, and I don't see any other reference

to it in the rest of these four paragraphs, but -- so just, I -- from the redline, it just sticks out, and that's the only change in that first paragraph, I believe.

A. (Williams) Thank you, Mr. Deveau. Just to reiterate what Ms. MacDonald was saying, it is just -- like, it's really just signifying more of a shift from having a bit of a balance with cloud and service providers with also Nova Scotia Power personnel as opposed to more of an nexus on cloud and service providers and less on Nova Scotia Power personnel.

Q. Okay.

A. (Williams) But to Ms. MacDonald's point, always relying on the diligence of our employees.

Q. Okay. And then in the fourth -- I think it's the fourth paragraph, the first paragraph at the top of the next page, I'll let you read that paragraph, and I'll just -- that highlighted section is a brand new -- was introduced to last year's version.

A. (Williams) Yes, sir.

[11:50:29] **Q.** So obviously it's the paragraph at the top of page 22 of 30 there, and it's the reference highlighted -- it's a reference to the Company maintaining cyber insurance coverage and the fact that subject to aggregate limits and depending on the scope and scale of impacts to the Company, they're more likely to be exhausted as a result of a sophisticated single cyberattack or if multiple events occur and that there was no guarantee that the Company will be able to renew such coverage on acceptable terms.

So is that a recognition of what happened in this particular case of why that language would have been added?

A. (Williams) Yes, sir. Without getting into the confidential nature of the attachment we referred to before ---

Q. Yes.

A. (Williams) --- which is CA IR-6, yes, this would be recognition of the experience we've had

over the last year and a half.

Q. Okay. And this is public information that's just ---

A. (Williams) Yeah.

Q. It's one of the many -- cybersecurity risk is one of the many risks that I suppose all the nervous accountants want to put in the financial statements of what risk can impact the company, and this is but one of them?

A. (Williams) Yeah, absolutely.

Q. Yeah. Okay. Let's get back to the policies. We talked about compliance. Now I want to talk about the policies themselves, and these policies -- the various policies were provided in Board IR-9 and in another locations as well, but they were provided in Board IR-9. We'll get to that. And they were filed confidentially, except for Nova Scotia Power's Customer Privacy Policy.

VICE CHAIR DEVEAU: So let's go to the

list there. It's -- Rob, it's Board IR-9, Exhibit N-10, and it's PDF page 28. So those are the documents that were provided the various policies, procedures and guidelines. There's 13 of them there. The last -- the thirteenth one is the only one that's non-confidential. It's NSPI's Customer Privacy Policy.

Can you bring up the next paragraph there? Can you show that in its entirety? Right there.

BY VICE CHAIR DEVEAU:

Q. So it says:

> To its knowledge, and based on reasonable inquiry, NS Power collected the personal information of its current and former customers in compliance with all applicable privacy legislation, including PIPEDA, and all other applicable law. Information about customers (both former and current) is collected in accordance with NS Power's public customer Privacy Policy...

So my question is, is it the Company's view -- I just want to confirm that the retention of the Social Insurance Numbers up to the time of the incident was in compliance with its legal requirements and

policies?

A. (Williams) Yes, sir. I think that goes to the -- I think I had the discussion with Mr. Mahody and perhaps others on the record where what is reasonable or necessary in the circumstances must be a contextual discussion or analysis. And when you're dealing with a CIS system, it is just that; it was not possible to delete those. So that would be the relevant caveat, I think. When you're reading the policies on their face, I understand where you're going with it, but when you understand it or discuss it in the relevant context, it becomes apparent that there can't be an expectation that you're doing something that is not possible to do.

Q. And when you talk about the legal requirements, you're talking about -- and the context; you mentioned the context -- that's based on the legislation that falls under the Office of the Privacy Commissioner, the federal office? That's what you mean, that

legislation? The context is from that legislation?

A. (Williams) That's under PIPEDA.

Q. Yeah, okay. At the very start of that paragraph, it says, "To its knowledge, and based on reasonable inquiry," and I'm not sure -- what did you mean -- what was meant with the words "and based on reasonable inquiry"? What did that mean? Because what you're saying is based on its knowledge and reasonable inquiry, NS Power collected this information from customers in compliance with the applicable privacy legislation. So what's this reasonable inquiry?

A. (Williams) It may be an unnecessary qualifier, sir. I think it's just really signifying that when you're making absolute statements about vast amounts of information in general, yes, everything was collected. Was every single -- could there be one instance over the last 30 years where something was collected that wasn't necessary? That's possible. But like I said, it's probably an unnecessary qualifier, but

the statement stands and would stand without it as well.

Q. Okay. One way I read it was that -- was it based on reasonable inquiry of customers, and they provided -- because you mention at the end of the paragraph that the matter is collected -- the information is collected in accordance with the Privacy Policy. I was just -- you mention elsewhere in the rebuttal that customers are aware of the policy; it's available -- the Privacy Policy is a public document that's available on your website. I was just -- I got the impression that perhaps you were putting the onus on customers that because there was a reasonable inquiry or they set up an account and that the Social Insurance Number was provided on that basis, that that somehow legitimized the retention of the SINs. That's not what you meant? Basically, in totality, your practice is to follow the legal requirements. That's what you're saying?

A. (Williams) You summarized my view and our intention, yes.

Q. So going back to the list at the top of the page...

VICE CHAIR DEVEAU: And I'm sorry, can we go back to the question, Rob? Right there. I think it's the last -- I think it's (e), if I'm not mistaken. Yeah, just go down a bit. Okay, right there, page 1 there of 4.

> A copy of the key policies, standards and guidelines under this framework at the time of the Incident have been provided as listed in the table below.
>
> So let's go back to the list.

BY VICE CHAIR DEVEAU:

Q. Have any of these policies been revised since the incident?

A. (Williams) Yes, sir, they're in the process, and I think we speak to that in the rebuttal. So we've had all of these -- the policy and the procedures have been reviewed by Gartner as an external consultant.

Q. Right.

A. (Williams) And then those -- the

result of that review had been included in the third-party review that's being undertaken, or the audit that's been undertaken through the OPC process.

Q. Right. But have they been adopted by the Company yet?

A. (Williams) They have not yet because we're waiting for the outcome of that process.

Q. Okay.

A. (Williams) So rather than roll out those policies and procedures now, and then again once we get the feedback from LevelBlue, the decision was made to roll it out once.

Q. Okay. Before the incident, before -- yeah, before the incident, how often were the -- these policies reviewed? Was there a set review every number of years, or...?

A. (Williams) These policies and procedures, I believe our version dated as -- they're confidential, but I'm comfortable saying that I believe is

2020, that the date on their last reviewer. They would not have been reviewed in the interim between 2020 and now, just because there would not have been a general reason to. They would have been set ---

[12:00:03] **Q.** Yeah.

A. (Williams) --- based on the existing legislation that had not changed or evolved.

Q. Right.

A. (Williams) But now we're in a position, as we talked about ---

Q. There -- there's new legislation ---

A. (Williams) --- there's new federal legislation.

And I think in addition to that, the other factor that is significant is the adoption of AI and how that can influence the sphere. So recognizing the proliferation of AI and those types of technology, like that, even absent the federal legislation, would have

justified reviewing these.

Q. Right. But it's your view that these policies at the time of the incident did comply with the applicable privacy legislation.

A. (Williams) Absolutely, sir. I believe that's consistent with Ms. Ralph's evidence as well ---

Q. Yes. Yeah, yeah.

A. (Williams) --- (inaudible due to speaking over each other).

Q. Okay. Now, actually what you volunteered I was going to ask you as the next question. I realize it's confidential, but I was going to ask you if I can ask about the last update indicated for these policies.

So you mentioned 2020. I think generally they were 2019 to 2021, and there was one in 2025. Does that sound correct?

A. (Williams) Yeah.

Q. Okay.

A. (Williams) So I certainly take you -- take your word for that, sir.

Q. Yeah. Okay.

I'll take you to the rebuttal, N-17, page 10 and 11. And I think it's the same sentence that Mr. Melanson took you to this morning; it's similar. It is line 25. It may not be the same passage, but it's essentially the same issue, same sentence:

> At the time of the Attack NS Power had a common set of cybersecurity standards and policies that are informed, in part, by the...(NIST) Cybersecurity Framework in place. Furthermore, the [Board] regularly reviews and makes continuous improvements to its cybersecurity programs to ensure it was and continues to be in line...

We'll just go to the next paragraph:

> ...with the latest guidance.

It says:

> In connection with these efforts, [Nova Scotia] Power has recently completed an extensive two-year update to its...practices to comply with current policies and anticipated changes in standards communicated

by NIST.

My question was a different question. As a result of this two-year update, there were changes to practices, but the policies that we've talked about just now, the 13 policies, those policies were not changed; correct, as a result of this two-year review -- two-year update?

A. (Williams) Yeah. They would not have been, and important to realize. So the review we're referring to here on page 10 and 11 relates to cybersecurity standards and policies, not ---

Q. Right.

A. (Williams) --- privacy ---

Q. Not necessarily privacy?

A. Not necessarily ---

Q. Okay.

A. Not necessarily, not at all privacy policies ---

Q. Okay.

A. (Williams) --- and procedures.

Q. Okay.

VICE CHAIR DEVEAU: So let's go back to that list of policies, Rob.

MR. NORWOOD: (Inaudible due to away from microphone.)

VICE CHAIR DEVEAU: Sorry. It was -- it was the -- right there, yeah. It was Board IR-9, Exhibit N-10.

BY VICE CHAIR DEVEAU:

Q. Those 13 policies, 13 of them are marked -- sorry. Yes. Nine of them are marked as being NSPI policies, and the other four, there's no indication of who the policies belong to. It's -- these are confidential.

Can I ask who the other -- what the other four policies belong -- who they belong to?

A. (Williams) Yes, sir. They all belong to NSP.

Q. To who?

A. (Williams) They're all Nova Scotia Power policies. They're just -- awkward way of labelling them, perhaps.

Q. Okay. I actually read a few of those policies not being a Nova Scotia Power policy, they were Emera policies.

A. (Williams) They are policies that would have been jointly developed with Emera and other of its affiliates, but they would be developed specific to Nova Scotia Power. So ---

Q. They would have been non-specific.

A. (Williams) Specific. Specific ---

Q. Specific to Nova Scotia Power?

A. (Williams) Yes. I mean -- so as an example, Emera, as a company, would not have the same privacy requirements as ---

Q. Correct.

A. (Williams) --- Nova Scotia Power.

Q. Yeah.

A. (Williams) So these are -- while they are on some of the headers, at least without going through them all, they're -- there's an Emera logo. They are Nova Scotia Power policies, and they refer to the Emera company, meaning the affiliate company, ---

Q. Yeah.

A. (Williams) --- Nova Scotia Power.

Q. And just to that point. Nova Scotia Power and TECO, for example, first of all -- well, first of all, they operate in two different -- entirely different jurisdictions, but they would have different privacy needs in terms of the amount of personal information than NSPML would or Emera Energy in terms of privacy, personal information?

A. (Williams) Yes. And to the extent that (inaudible due to speaking over each other)

would even apply to ---

Q. Right.

A. (Williams) --- certain of those ---

Q. Right.

A. (Williams) --- (inaudible due to mumbling), yes.

Q. Okay. So even though they're confidential, can we identify the two that I have that are Emera?

A. (Williams) Yeah, I'm happy to have kind of high-level discussions ---

Q. Okay.

A. (Williams) --- that will ultimately be helpful, yeah.

Q. Okay.

A. (Williams) Yeah.

Q. Have the discussion in a confidential session?

A. (Williams) No. I mean ---

Q. Oh.

A. (Williams) --- they're confidential so that ---

Q. The contents, not ---

A. (Williams) Yeah.

Q. --- the description.

A. (Williams) Exactly. So I'm comfortable where we are right now ---

Q. Okay. Yeah.

A. (Williams) --- in continuing this type of discussion.

Q. So I have number -- so I have number 2, the Collection of Personal Information Procedures. I'll let you bring that up.

A. (Williams) Yes, sir.

Q. So it says Emera, but then it does say, "Adopted by all Emera affiliates," so that's how it applies to Nova Scotia Power?

A. (Williams) That's right. And as I said, this -- while it has Emera, this would not even apply to Emera because they're not collecting personal ---

Q. Right.

A. (Williams) --- information.

Q. Right. Okay. And then -- and then the other one I had was number 9, Information Management Policy. PDF 90, yeah, number 9.

And that one, it actually -- it says, "Adopted by Emera". It says the Emera company, but there's no reference to affiliates or anything, but...

A. (Williams) Yeah. So this is a -- somewhat of a different format, but the same thing, and I can confirm that this is ---

[12:09:50] **Q.** Same intention?

A. (Williams) --- this is Nova Scotia Power's written policy, yes.

VICE CHAIR DEVEAU: The one that is public, the Customer Privacy Policy -- Rob, that's PDF

page 43.

BY VICE CHAIR DEVEAU:

Q. That one, I do not see -- I didn't see a date on it when it was last updated.

A. (Williams) I'm not aware of a date on here, sir. And the reason for that is this is not a document in the same way that the others are. This is basically a screenshot from our web page.

Q. Okay. So that one would have been in effect -- well, you mentioned it was in effect in -- at the time of the breach; it would have been in effect before that as well? No significant updates for the last few years?

A. (Williams) That's correct.

Q. Okay. Let's go to rebuttal N-17, page 18, line 21. Yeah.

So that's -- we've talked about that information protection audit of Nova Scotia Power's Data Lake was conducted in December 2024 as part of the

company's annual audit program.

And I recognize in the previous paragraph, you referred to -- you wanted to make a point of clarification in relation to the response you gave to INQ Law's IR-2 that asked for private audit plan and dates of audits of access to personal data of customers implemented by Nova Scotia Power in the two years leading to the cybersecurity incident.

So generally, the response in that IR -- we can bring it up if you wish -- but it was that there were none. But afterwards, you wanted to make this distinction.

But the audit -- like when -- on line 21 when you talk about the company's annual audit plan, that's -- program, sorry -- the audit program, that's in relation to an audit of access, reviews of access to information on your system.

That's not in relation to an audit of the compliance or an audit of the policies themselves;

it's an audit of access to information that is made -- that is made in the organization; correct?

A. (Williams) The specific reference to "Audit program," so audit program is referring to the company's annual audit program. That's the program that's established ahead of time on an annual basis as to what the -- typically what will be audited through that time period, that year.

Q. So not just -- not just privacy policy.

A. (Williams) Not just privacy.

Q. It could be anything.

A. (Williams) That's audit -- that's the overall audit program and new audit programs.

Q. Is that the financial audit, part of the -- or no?

A. (Williams) It would include any aspect of the company that the audit function -- it's not a management decision. It's the audit team's decision as

to what that ---

Q. Internal audit team, or...?

A. (Williams) Yes.

Q. Okay. Okay. So that can relate to anything at all in the company, purchasing and ---

A. (Williams) So I don't want to -- in fairness to that team, I don't want to give the impression that it is randomized.

Q. No, no, no.

A. (Williams) There's a ---

Q. No, I realize that.

A. (Williams) Yeah. But yes.

Q. So it's not just -- it's not just -- but it's not just access to information -- access to -- you know, whether there was unauthorized access. It's audit about ---

A. (Williams) There's probably an infinite number of examples we could give.

Q. Right. Right. Okay.

But as we discussed earlier, there's no formalized review of compliance or the policies themselves on a regular basis, on a regular cycle; it depends on what the internal audit team decides.

A. (Williams) Yes, so they may have a specific cycle in mind ---

Q. Right.

A. (Williams) -- but it's not something that management is involved with intentionally.

Q. Who's part of that audit team? Is it a -- like, a financial people or ---

A. (Williams) It's a specific audit team. It's an Emera audit team that audits affiliates.

Q. Okay.

VICE CHAIR+ DEVEAU: In the customer policy -- let's go back to that customer privacy policy, Rob, PDF page 45 of that. It's the IR.

Yeah, PDF 45.

BY VICE CHAIR DEVEAU:

Q. So this is a public Customer Privacy Policy. And it's -- it's under "Correcting and retaining information" at the end.

It says, in the second paragraph under that heading:

> The length of time we keep your information varies depending on the product or service in question and the nature of the information. We have retention standards that allow us to meet customer service, legal and regulatory needs. As a result, it may be necessary for us to keep some of your information on record even after the end of your relationship with us. When the information is no longer required, it is destroyed or anonymized.

So I guess my question is simply when the incident happened at the time of the breach, your statement there was not correct, right? It was -- the information when no longer required had not been destroyed or anonymized.

A. (Williams) Well, I struggle with that word as well, sir.

I will say it was accurate as it

related to CIS because of the discussion we had previously about what is possible. When we talk about that Data Lake and what resided in the staging area, that data was no longer required there and it had been retained as we discussed yesterday.

Q. Okay. We'll move on, as Monty Python used to say, and now on to something completely different.

We'll deal with communications.

And it's generally in relation to the -- the script we talked about this morning for TransUnion, so it's Exhibit N-10, response to Board IR-14, PDF 60. And it's lines 10 to 15.

Yeah. So it says there:

> Customer care associates were provided with key messages and speaking points. [Second line] This included an extensive Frequently Asked Questions resource that detailed our latest response to the incident, including the customer notification process and the offer for free credit monitoring service. This FAQ Guide was developed with TransUnion to ensure customer interactions were empathetic, accurate and consistent.

Just my question -- and the question is premised; there are 36 questions there in the Frequently Asked Questions. And I only saw eight of the 36 questions that referred to credit monitoring.

So in that context, I was wondering why TransUnion was involved in the development of the FAQs, generally.

I can see them perhaps being involved in the FAQ section, but I would have thought -- many of those questions related to the breach itself. I would have thought Nova Scotia Power would have been in a much better position to answer those particular questions, and then you could have been, "Empathetic, accurate and consistent."

So I'm just wondering why they were developed with TransUnion and not by Nova Scotia Power.

A. (Lanteigne) Thank you for the question, Mr. Deveau. I -- just to really clarify. So

the questions and the scripts that the TransUnion representatives would have had, TransUnion would have had a hand in helping us with that information, but there would have been other parties, including Nova Scotia Power, that did contribute to the development of that.

So TransUnion obviously brings in the expertise in providing the myTrueIdentity service, and also has supported incident responses before, so they would have reviewed the information and provided their input on it, but we would have handled questions specifically to Nova Scotia Power of that development.

[12:20:12] **Q.** Sorry; you would have handled or prepared the answers for the other questions, you mean?

A. (Lanteigne) That's right. Like, ---

Q. Oh.

A. (Lanteigne) --- it would have been -- it wasn't a TransUnion -- the document was not all created by TransUnion, but they did have some input into

it.

Q. Okay. So recognizing their expertise, for lack of a better word, in terms of the credit monitoring and the incident response, they would have helped you on those parts, but the rest of it, it was Nova Scotia Power.

A. (Lanteigne) Nova Scotia Power, and advisors that we had ---

Q. Yeah.

A. (Lanteigne) --- secured as well ---

Q. Yeah.

A. (Lanteigne) --- participated in that creation, yes.

Q. Okay. Let's go to Question 26, which is PDF 69.

VICE CHAIR DEVEAU: Sorry; the prior page, Question 26. Yeah, at the bottom. And just put the very top of the next page. Yeah, right there.

BY VICE CHAIR DEVEAU:

Q. So the question was, the customer asked, "I want to speak with someone at Nova Scotia Power." And the response from TransUnion...

Perhaps before we go there. When were these FAQs generally prepared? So I assume when the -- well, when were they generally prepared?

A. (Lanteigne) I think they would have first been prepared in advance and at around the same time as the letter in May being issued to customers.

Q. Right, okay. So the letter would have been May 10th. So in that timeframe, May 13th, when customers received this, in advance of that letter you would have been ready with these FAQs because you were going to start getting calls. Correct?

A. (Lanteigne) That is correct.

Q. Okay. And -- so Question 26, it says, "I want to speak with someone at Nova Scotia Power." And it says:

Nova Scotia Power takes this matter very seriously. To assist you with any questions you may have regarding this incident, Nova Scotia Power has established this contact centre to address your questions related to this incident.

And at the top of the next page, part of this question -- and that's the end of it, there's nothing more after that.

VICE CHAIR DEVEAU: Rob, you can go down a bit.

BY VICE CHAIR DEVEAU:

Q. But it says, "If caller pushes, escalate." So there was no -- there was no offer on TransUnion's part, as part of the script, to say, "We will -- we can escalate it to Nova Scotia Power if you wish." It was TransUnion's decision to escalate.

I suppose one of the triggers would have been the customer saying, "I want to talk to Nova Scotia Power. I don't want to talk to you." But it -- was there any script -- I didn't see any -- that said,

"You can have your matter referred to Nova Scotia Power"? It was just through TransUnion that it was done?

A. (Lanteigne) Yeah. So that -- a couple of things. So -- and I believe we talked about this yesterday, but if a customer during this timeframe had called Nova Scotia Power directly, Nova Scotia Power would have been able to assist customers, and our customer service associates did have the Q&A as well.

Q. So on that point. So the number on the letter was different than your own customer centre.

A. (Lanteigne) That is ---

Q. Those remain two distinct. Okay, that's ---

A. (Lanteigne) That is correct.

Q. Okay.

A. (Lanteigne) And the purpose of establishing the centre at TransUnion that had this -- these questions that we're looking at was just to ensure that we could have the capacity to support questions that

were coming in, again recognizing TransUnion is a -- is an expert in this space. So the questions were designed in a way to help answer questions for customers who had questions about the incident specifically. So the script that was provided to TransUnion, and this question in particular, was really just to, you know, emphasize that key point, that we do take this matter seriously.

If the customer wanted to talk to us, they did have two avenues. They could call our customer care directly, and then the second one was the escalate that's listed after the question, that just meant that the customer's request was specifically sent to our team and we would follow up and call that customer back to talk to them about their specific concerns.

Q. Right. But TransUnion would have to have reason to escalate or an impetus to escalate, I suppose, if some customer said, "I want to talk to Nova Scotia Power, I don't want to talk to you." Right?

A. (Lanteigne) Yeah. If a customer

-- if a customer persisted, and they wanted to talk to an actual Nova Scotia Power employee, that's where it would have come back to us ---

Q. Okay.

A. (Lanteigne) --- to have the conversation.

Q. Okay.

VICE CHAIR DEVEAU: Thank you. Those are all my questions.

QUESTIONS FROM THE CHAIR

Q. The ground's been pretty much run over by the time it's gotten to me, but -- and I'll try not to be overly duplicative. There's probably a couple of horses I might want to poke just to make sure they're dead, though, so just please bear with me.

THE CHAIR: Mr. Norwood, if we could first turn to Exhibit N-17, page 53 in the PDF, please.

BY THE CHAIR:

Q. Focusing on the paragraph that begins at line 17. So the paragraph states:

> More specifically, there were three systems where personal information was retained for longer than the timeframe set out in the retention schedule and which resulted in the exposure of customer information as a result of the Attack.

In terms of the three systems, I just want to make sure I understand what we're talking about. So there's the CIS that you referred to, although you've indicated that that really wasn't involved in the attack,

so that really wasn't a source of personal information.

A. (Williams) Well, it was just -- it was a source in that the information originated there. But yes, sir, I think you've -- you understand it.

Q. Okay. And then the copy that was in the Data Lake was the second source. Was that the only source of personal information that was accessible in the Data Lake?

A. (Williams) That's my understanding, is that that information or that data in the staging area, for the reasons that we've discussed previously.

Q. Okay. But in terms of the potential access to personal information, that was the only, I'll call it a file. I appreciate it's probably more complex than that, but that was the only file that was able to be accessed that had personal information on it in the Data Lake?

A. (Williams) Mr. MacLeod is just

noting that to the extent there may have been anything in there that hadn't already hit the 14- or 90-day retention. But I -- for the purposes of this discussion, I -- yes, your understanding is correct.

Q. Okay. And the third source, as I understand it, was a Network Attached Storage device?

A. (Williams) Yes.

Q. And so to the extent that personal information was impacted, I think is the word you've been using, it's really either from the Data Lake copy or the Network Attached Storage device?

A. (Williams) That's right, and the overwhelming majority of that is, obviously, the Data Lake, as we've been discussing.

Q. Okay. And the paragraph, the way it's written, it refers specifically to personal information -- sources the:

> ...personal information was retained for longer than the timeframe set out in the retention schedule...

I take it it's the same whether it was longer than the timeframe in the schedule or shorter than the timeframe in the schedule. That's where the source of all personal information that was from, those three sources?

A. (Williams) Can you just maybe give that to me one more time.

Q. Yeah, I didn't -- I didn't get that out very clearly. But it says there were three systems where personal information was retained for longer than the timeframe set out in the retention schedule.

My question is, really, that wasn't intended to limit that statement. The three systems where personal information was available to retain, that's what it was. It wasn't just something about being longer than the timeframe and the retention schedule.

[12:30:11] **A.** (Williams) So I just want to make sure I give you an accurate answer, sir, because -- but I think the answer is yes to your question, but could you

just maybe try it one more time to make sure I have it right?

Q. Yeah, sorry. Sorry.

A. (Williams) No, it's just as much me, I'm sure.

Q. Yeah. So I'm just getting -- I'm just getting tripped up and, unfortunately, I'm tripping everyone else up over the wording here that just is focused on personal information retained longer than the timeframe. And I just want to be clear that that's not intended to limit that statement in any way.

If I were to take those words out and say there were three systems where personal information which resulted in exposure of customer information, it's the same thing.

A. (Williams) Yes.

Q. Yeah, okay. Thank you.

Sorry about that.

A. (Williams) We got there together,

sir.

Q. Okay. In terms of the data that was in -- the copy that was in the Data Lake, is it a fair characterization to say that Nova Scotia Power was not aware that that copy existed at the time of the cyberattack?

A. (Williams) Yes, that's a fair characterization.

Q. Okay. And you sort of explained the 14 and 90 days -- I was going to ask about. You responded to the Vice Chair about that.

As I understand it, once the -- once this data that was intended to be used in the MyEnergy Insight was used, it should have only been there for 14 more days at the most.

A. (Williams) Yes, that's my understanding of the delineation between the two. Once it's been manipulated, it's subject to the 14 days. If it has never been manipulated, then it's subject to the 90.

Regardless of whether it's used or not, it's gone within 90 days.

Q. And there's a -- there's a phrase in N-17 -- and I guess we can pull it up if you need to. It's actually just on the next page if we want to scroll down to line 22 there.

> Work streams in the Azure Data Lake, including in the staging area, were automatically cycled through the age of information...

The 14 and 90 days you just talked about.

It goes on to talk about the "Automatic setting must be manually engaged..." It doesn't really sound like an automatic setting if it has to be manually engaged, so if you could kind of tell me exactly what's going on there, I'd appreciate it.

A. (Williams) So again we're getting close to the limits of probably my expertise, but -- and I don't want to leave you the impression that it's pulling a

lever to -- it's not manual in that sense. It's coding it in, so coding the automation in, so manually coding it in would be my understanding, sir, but we are at the cusp of my expertise on this.

So there is an automation to it. We do know that that automation was in place and functional and working in all other areas of the Data Lake but for the furthest one.

Q. And in terms of -- so it's coding, then. I was envisioning going and making a system setting or checking a box or something. It sounds like it's a little bit more complicated than that. It's fine. It doesn't matter.

It required someone to take that physical step of doing that?

A. (Williams) Yes, and you've probably exposed the limitations of my knowledge, whether it's coding or -- but there is something that needs to be positively engaged by an individual.

Q. And given the sensitivity around cybersecurity and personal information, what are the fail-safes that Nova Scotia Power has to take out or check that opportunity for human error?

A. (Williams) Sorry, sir. Could you just give me the question -- I think I generally get it, but can you give me the question again?

Q. I'll try to break it down a bit more simply.

So someone made a mistake in terms of when they put the data in the system, they didn't set it up appropriately to be automatically removed; correct?

A. (Williams) That's our understanding, yes.

Q. And so what safeguard do you have to take out the opportunity for a human to make that mistake?

A. (Williams) So this -- so I don't know from a cyber perspective what is in place. An

example of a safeguard, though, or a measure is the Data Lake audit that we've been referring to, and that is on the record.

As part of that audit, there is an assessment of whether the appropriate controls were in place within the Data Lake, and that's one of the reasons why we know that the appropriate controls were in place within other aspects of the Data Lake.

Q. Can you explain why Nova Scotia Power remained unaware for three and a half years that data existed in the staging area?

A. (Williams) So I'll ask you to -- just so I'm answering precisely, I'm going to ask you to give it to me again, sir.

Q. Why didn't Nova Scotia Power know that that data still existed in its system for three and a half years?

A. (Williams) So the reason we wouldn't have known and the next -- within the next

process, they may be able to shed further light on this in terms of the technical aspects of it. But the reason we wouldn't know at this point is because -- because that process was not engaged. The assumption would have been that it was engaged. And the audit function that was performed and assessed, at least in part -- the Data Lake and what functions were performed within the Data Lake, confirmed that the appropriate functions were in place within the Data Lake.

Obviously, the scope of that audit did not include this particular workstream and this particular staging area, but it did assess other areas of the Data Lake and confirmed that those processes were in place.

So I can confirm for you that we did not know. Precisely why we did not know, it's a failing of those two things.

Q. So it's safe to assume that there was no audit or check of what information was in the staging area in three and half years -- at least three and

a half years?

A. (Williams) Yes, sir. That would be my understanding, that there was not an audit that specific -- the scope of which specifically would have encompassed this aspect of the Data Lake. But as I said, there -- the audit that we do have on the record and that we are aware of, it did encompass other aspects of the Data Lake.

Q. So I'm getting the sense, and correct me if I'm wrong, that Nova Scotia Power was relying entirely on the fact that this information had a set period where it was supposed to be deleted, 14, 90 days, and there was not much else that was done to verify that.

A. (Williams) Well, there was the audit -- the audit function that was in place as well, and it was auditing whether those retention periods were being fulfilled within the Data Lake because, as I said, obviously that scope of that audit did not encompass this

specific workstream or storage -- or staging areas.

Q. Were there any audits done between 2021 and 2024 other than the one that's disclosed in this proceeding of the Data Lake?

A. (Williams) That's the only one that I'm aware of, sir.

Q. So moving on to the Network Attached Storage device, my understanding, which is probably less than yours, Mr. Williams, about this is that that, from a user perspective, operates essentially like a shared network drive. People can access it to save files there and depending on their rights, could move and delete and so on, but that's basically something you would see on your laptop in a network drive that different people have access to?

[12:40:31] **A.** (Williams) Yeah, I think that's generally correct. Different drives would have had different degrees of sharing within them, but yes, generally, that's correct.

Q. And what personal information was stored in the Network Attached Storage?

A. (Williams) So just to be clear, there was nothing -- there was no personal data stored within -- there would have been information included in those drives and one-off information that if someone had been doing a report on something or there would have been a draft response on something, there would be potentially one-off versions, but nothing was stored as you would think of it in CIS or what occurred in Data Lake.

THE CHAIR: So, Mr. Norwood, if we could go to page 55, next page, line 2, please?

BY THE CHAIR:

Q.

> The NAS was a dedicated storage device that enables multiple users to store and share files from a central location. The NAS contained millions of files supporting various aspects of NS Power's operations and business, including some employee and customer information.

I'm assuming that millions of files are on that system. Some of them have been sitting around

for a while?

A. (Williams) So I don't know -- just one sec. So I think I'll maybe start again. So your assumption would be correct, and that's why it's been identified here, because NAS was a system where there wasn't the ability to automate that removal, and as is explained here, it was -- there was the planned shift or evolution to SharePoint Online and remove the NAS entirely and then automate the ability to both scan and remove for any personal data that was uploaded to that system. So yes, there could have been personal data that was on there, and that's again why it's been identified in the evidence.

Q. And in terms of the ability to automate the removal of that sort of information, I understand the explanation for the CIS, it's a particular system that's set up in a certain way and would involve a lot of coding. The system that we're talking about here, which is akin to a network drive, a shared network drive

that has files and folders, is the technical difficulty the fact that you have multiple users and millions of files who have stored and created and put information on this system over a number of years in a relatively unorganized way? Is that the technical difficulty?

A. (Williams) So I would say yes, sir, and that's, I think, in essence, what the modern SharePoint Online addresses, where you have the ability to not just scan and automate the removal but you're also categorizing the type of documents that are going on there. So you have a much better understanding, a much better way of organizing the data that's on a system like that. The NAS is not to the same extent as CIS, but it is just another example of a system that has now been surpassed by superior technology and is, I think, just emblematic of the evergreening and evolution that occurs when you're dealing with IT and the privacy implications that come with it.

Q. The Company's preferred means of

dealing with information like would be stored in the NAS now is SharePoint?

A. (Williams) I'm just hesitant on the "preferred". It is -- I mean, our employees would have the ability to also use MS365 OneDrive, but with that, that is newer and that has the ability to scan and doesn't have the same technical limitations. So in terms of sharing documents that would be available to multiple people in the company, yes, the preferred approach is SharePoint because of the ability to categorize those documents and organize it. OneDrive is more of a convenience working within a very small group or within a couple of people. SharePoint is where the majority of documentation would be included.

Q. And were either SharePoint or OneDrive impacted by the cyberattack?

A. (Williams) No, they were not.

Q. And how long has the Company had SharePoint?

A. (Williams) SharePoint -- there's iterations of SharePoint. So SharePoint has been used by the company for a number of years. SharePoint Online is the version that has the availability to do the things that we've been talking about. There's been prior versions of SharePoint that have not had that ability.

Q. And how long has the Company had access to either SharePoint version?

A. (Williams) We've had a version of SharePoint. I don't know definitively, sir, but certainly going back prior to 2020, 2018, 2019.

Q. So ---

A. (Williams) Sorry, sir, I'm being reminded that our on-premises SharePoint, so not the SharePoint Online, but our on-premises or previous version of SharePoint was impacted by the attack. It was not -- the information on it was not accessed, but the functionality was impacted in that we could not use it.

Q. Has that been regained? Do you

now have access to the data that's on there now?

A. (Williams) In large part, no. It just goes to how crippling this really was. So from the regulatory perspective, that is how we operated and prepared documents. So all of a sudden, on April 25th, we no longer had any of the documentation we had historically or anything that we were preparing for filings with the regulator. So everything had to be migrated to the SharePoint Online on the fly, effectively.

Q. For the Network Attached Storage, the use of the Network Attached Storage device, does the Company have any particular policies about how that should be used and what information should be put on it?

A. (Williams) Yes, so it has our existing -- we have our existing policies and procedures, and then we have the training that exists for our employees, but that is the problem with the NAS; beyond that, there's no way to control how it's used or what's being put on there, and that's one of the reasons that we

had plans in place to move away from it and destroy it, because of the limitations that it has in that regard and our inability to control it. The SharePoint Online has much more -- many more capabilities than obviously the NAS, but also more so than the previous version of SharePoint, which I believe is SharePoint 2016.

Q. When we started this line of questions, we had a bit of an exchange about whether the information was supposed to be stored on the NAS or not and hold up to reference to the millions of files. Your initial response was, "No, that was intended for storage. It was for transfers or whatever." Was it the case that this was only supposed to be for temporary sharing and use and that information should have been deleted after that was done?

[12:50:00] **A.** (Williams) So, you know, originally, I don't -- I don't have any experience as to what originally the Network Attached Storage would have been established within Nova Scotia Power. It had evolved

to a point where it was used commonly with people but not necessarily to collaborate on documents. SharePoint was the preferred and has always been the preferred manner in which to do so, but that is not to say that the NAS, Network Attached Storage, could not or was not used for purposes in certain instances, but again, when documents would be shared internally, they would be shared through SharePoint, with links through SharePoint or the documents being sent through SharePoint.

Q. Did the Company consider it to be acceptable practice to allow personal information of customers to be copied there and not removed?

A. (Williams) No, it would not have been acceptable practice for that information to not have been removed, but there was no way to, as I say, scan and automate that removal. And so you would have -- you would certainly have instances where employees depart, they move on, they're in different roles, and data is perhaps left behind.

Q. And I know you've said -- or the Company has said that it had a plan in place. It's referenced on the page and it's still up on the screen in the next paragraph down, beginning on line 7. They had a place -- a plan to provide the business owners, I guess, an opportunity to remove that material from the Network Attached Storage device within a certain deadline that hadn't -- the trigger hadn't been pulled on that? That was just in planning?

A. (Williams) That plan was part of the shift to SharePoint Online, the intent. So there was a plan to move from SharePoint 2016 to SharePoint Online, and as part of that, we would obviously be doing away with SharePoint 2016, but you would also do away with the NAS.

And as part of that shift, the instruction was expected to be, "You're going to lose everything on the NAS, so if there's anything you need from there, take it off and put it on SharePoint, and if there's any personal information there, it needs to come

out." But that was the plan and the path.

Q. And, sorry, that occurred in 2024-2025?

A. (Williams) No, that was in progress, and so not to dwell on -- the Emera affiliates were all making that transition at the same time, and certain of the Emera affiliates had already completed that transition. Nova Scotia Power was essentially next up in line when the incident happened. That's one of the reasons we were able to get back up and operational so quickly, because SharePoint Online was -- we were kind of next in the queue to do that, and so it was available to us to adopt immediately. So we really just escalated that transition process in the aftermath of the incident.

Q. And why wouldn't that sort of a process have been undertaken, going as far back as 2020, when SharePoint was first acquired or, you know, it was around then that I think you said for the previous version, the on-premises version?

A. (Williams) Yeah, it's just they evolution of a functionality within those versions. And so SharePoint online was the version where that was available. In 2016, that wasn't something that was part of the standard SharePoint offerings, those types of packages, and so SharePoint 2016 was an on-prem service. SharePoint Online was the first in the cloud version of SharePoint.

Q. My question is that the decision to migrate data from the Network Attached Storage to SharePoint Online, why wouldn't that have been done with the previous version of SharePoint, the SharePoint on-premises version?

A. (Williams) It would have -- we would have still had the same issue, and that was the SharePoint 2016. We would have been limited in what we could do in terms of scanning and removing. So SharePoint Online was the first version where that could be automated within that. So you could have done it, but you would

have had the same residual problem.

Q. There have been undertakings about the size of various data storage areas. I would ask a similar undertaking to understand what the size of -- the volume of data in the Network Attached Storage device was at the time of the cyberattack, if I could?

A. (Williams) Yes, sir.

THE CHAIR: So that will be Undertaking U-15.

UNDERTAKING U-15 - To provide the size or volume of data contained in the NAS device at the time of the cyberattack

BY THE CHAIR:

Q. In terms of the removal of Social Insurance Numbers, I'm going to characterize it as a relatively passive approach was taken in 2018. You might disagree with that approach. A change was undertaken in 2024 when more proactive steps were taken than to remove

the Social Insurance Numbers from the CIS at that point in time.

I think, Mr. Williams, it may have been you in some of the previous responses had talked about assessment of risk over time and changing assessment of risk, and I'm wondering if you can give me a bit of a better insight in terms of how the risk calculus changed between 2018 and 2024 that caused you to do it at that point in time?

A. (Williams) In terms of the initial approach, sir, I would characterize it as cautious more so than anything, but I don't know that I have much more to offer other than it was an evolving discussion, recognizing the risks of CIS. I think at the same time there was also ongoing discussions and development of a timeline for when the new CIS would be brought forward. And so there's a number of different things that I think came into play during that period, and I acknowledge the passage of time between 2018 and 2024. The reality is I

don't have much else to offer other than it's my understanding -- it's our understanding that what transpired during that timeframe was the continuous discussion of the recognition that the SINs needed to be removed and the continuous internal discussion or debate about what the risks were to CIS and what was an acceptable level of risk and what was the best way to go about potentially removing, isolating or identifying, I should say, and removing the SINs within that system.

Q. A moment ago, you connected part of that response to the timing of the replacement of the CIS. Does that mean it became apparent to Nova Scotia Power or that Nova Scotia Power made a decision at some point that because the CIS replacement project was continuing to be delayed, that perhaps more urgent attention to this Social Insurance Number issue was warranted?

A. (Williams) I don't think it would have been a -- necessarily a significant driver, sir, but

it would have been part of the discussions to what's the timeline on the replacement CIS where we're going to have the ability to automize this type of removal. And so when you're talking about is it worth the risk of doing the work within the existing CIS, you would want to understand the timeline in which you're going to have the ability to do the work in a safer environment or do it as part of a transfer to a safer environment.

[1:00:04] **Q.** You said earlier today, the policies, the current policies that you have around privacy were all developed around 2019, 2020. The retention schedule that goes along with that, was that developed at the same time?

A. (Williams) Yes. My understanding is that it would have been -- I mean, all relative, I suppose, same general timeframe. I think it would have been something that was beginning to be developed earlier than that, and I think some of that work would have likely occurred in the 2018, maybe in the -- a bit earlier than

that. But it would have been as part of the same initiative, yes.

THE CHAIR: Probably, I'm going to go for a while still, I suspect, so it's probably a good idea to break for lunch for now.

Any concerns if we shorten the lunch a little bit because of the longer break? Say 45 minutes, or so, instead? Seeing nods of general agreement, so we'll do that.

It's 1 o'clock now, or thereabouts. We'll come back at quarter to 2:00.

--- Upon recessing at 1:01 p.m.

--- Upon resuming at 1:46 p.m.

THE CHAIR: Okay. Welcome back.

GLEN MacLEOD, Resumed:

CHRIS LANTEIGNE, Resumed:

LIA MacDONALD, Resumed:

BLAKE WILLIAMS, Resumed:

QUESTIONS FROM THE CHAIR, (Cont'd)

Q. Just in terms of the Data Lake -- the data in the Data Lake, you'd previously noted that it was encrypted at rest. Does that -- that included the data in the staging area as well?

A. (Williams) Yes, sir.

Q. Okay. And is the -- does Nova Scotia Power pay a fee or a licence or anything maybe on a monthly basis based on the amount of data in the Data Lake? Is that how that works?

A. (Williams) I'd have to take that one away, sir, if you need an answer for that. No-one up here has a certain answer for that.

Q. Okay. If you wouldn't mind.

A. (Williams) Yeah, absolutely.

THE CHAIR: Undertaking U-16.

UNDERTAKING U-16 - To advise whether Nova Scotia Power pays any fees on a monthly basis based on the amount of data in the Data

Lake

BY THE CHAIR:

Q. I guess I'm just going throw this out here. I'm not sure who it's directly aimed at, but just in terms of the company's position, does Nova Scotia Power agree that one of the reasons to have a retention schedule and for destroying records after retention periods expire is to prevent theft, misuse, and unauthorized access, particularly in the case of personal information?

A. (Williams) We'd agree, sir, yes.

THE CHAIR: Mr. Norwood, if we could go to Exhibit N-16, please. Page 68 in the PDF.

BY THE CHAIR:

Q. In terms of -- I'm focusing on the paragraph that begins, "The types of impacted personal information."

In terms of the information that is included there -- and I probably should have pulled up the

other one because I'm going to include Social Insurance Numbers as well in that -- what is the retention period contemplated in the schedule for information of that type? Is it seven years?

A. (Williams) That's right, yes.

Q. And how long has it been seven years for that type of information?

I know we talked just before the lunch break that the retention schedule itself is circa 2020, maybe a little bit earlier. Did it exist even before that?

A. (Williams) My understanding, sir, is that there was a retention schedule prior to that. I don't -- I have never seen it.

I will say that it would have been very different, given the fact that there would have been more paper records at the time and that type of thing so that -- I mean, the world has changed, obviously, but I've never seen that retention schedule. But I certainly have

had it communicated to me that there was a prior retention schedule.

Q. Okay. And so it would have -- whatever the period would have been, it would included -- it would have included a set period for removing information like this from your records -- personal information of customers from your records?

[1:49:59] **A.** (Williams) I think it's safe to assume that, sir, but the retention schedule would have been a record retention, not necessarily specific to personal information.

THE CHAIR: And if we could go to Exhibit N-17 again. And going to page 53, line 8.

BY THE CHAIR:

Q. So:

> While Nova Scotia Power retained customer data beyond the timeframe set out in the record retention schedule, the retention schedule had been developed with specific technical functionalities in mind and strict adherence to it was not possible until those functionalities were in place.

That's been referenced a few times already in this proceeding.

It sounds like, though, that if the schedule was developed with those functionalities in mind, Nova Scotia Power, when it developed this schedule with the seven-year timeframe, would have been aware that it was holding personal information of customers already that was beyond that period at that point in time?

A. (Williams) Yes, that would have been the case in relation to the CIS.

Q. And what was the plan at that point in time to bring the company back into or put it into a place where it would be fully compliant with the -- what was contemplated in the retention schedule?

A. (Williams) So those measures would have been as we've discussed, sir, which would have been the understanding that in order to fully operationalize CIS so that it was consistent with the retention schedule; quite frankly, any retention schedule,

would have been -- would need to be -- it would need to be modernized. So that was the main strategy, if you will, to ensure.

And that goes back to the fact -- the discussion we had about the source. It is the source and it is what allows that information to persist within the system. Once you have addressed the source you have, for the most part, addressed the root cause.

Q. Okay. So what I'm not understanding from that, then, is that when the retention schedule was put in place, when the more recent iterations of the policies were developed, Nova Scotia Power knew it was holding onto personal information beyond those timeframes and essentially its plan was that the Customer Information System was going to be replaced and that was the solution.

A. (Williams) So yes, I think that is, in part, imparted.

I mean, we've also discussed, you and

I, about the evolution of SharePoint and the ability to automate within SharePoint, so -- and the effect that would have on the ability to then destroy the NAS, migrate anything from the NAS.

So there were -- there were those technological evolutions that needed to occur in order to fully -- you know, fully implement the schedule.

Q. The issue with the Customer Information System, would you agree, is a bit different than the issue with the Network Attached Storage?

As I understand it, the CIS, problem is that the way it's programmed, you're simply going to break it if you try to remove that data. The issue with the Network Attached Storage is more a human one: You have many people using it, they're not using it an organized way, and it's very difficult to police exactly what they're doing on it.

A. (Williams) Yes, I think that's -- yeah, I'd agree with that characterization. I think that

I would go back to the fact that the CIS is the source of that information for the most part. That's where the information originates and resides on the system, so I think that kind of proliferates out from there.

Once you address CIS, you have in part addressed, and I say in part the issue elsewhere, but there's also the need to ensure that those other systems, and in this case the SharePoint and NAS aspect of our systems is also in compliance.

Q. Right. But the NAS was not in any way dependent on anything having to do with the CIS and the fact the data had to be retained. That was just a function of it was there for people to use and they were using it, and perhaps not in a most data-friendly way.

A. (Williams) That's right, and it had no automation available on it. That's correct.

Q. Now, you've made an improvement, and I just wanted to ask about that because it's also referenced in N-17 at page 61, at line 28.

We can pull it up quickly. It's a reference to the scanning tool that was used to remove the Social Insurance Numbers, and there's a reference that once it's kind of -- you're comfortable that it's not -- no longer needed exclusively for that purpose it may be used to expand it to other personal information. And I just wondered if you could elaborate on that a little bit.

A. (Williams) So it's a newer tool that's now available within 365. So that -- I think I mentioned it just in passing earlier. So it's a newer tool now being scanned -- used to scan for SINs on an ongoing basis. And as we get additional experience with it, it will be expanded to scan for all types of personal information.

Q. And I'm just trying to picture this in my mind. So it would scan within your systems for personal information in that sense, and if it detected any it would produce a report that would go to someone?

A. (Williams) Yeah. So I'm not

entirely sure on what the output of it is, but it doesn't -- just to be clear, it scans the Microsoft systems, not the entire systems, which would include Outlook email, those types of things.

Q. And SharePoint and OneNote?

A. (Williams) Yes. Yes, yeah. And so would identify those. I can't confirm precisely what the output is, but yes, it does flag and allows for that information to then be addressed.

THE CHAIR: Mr. Norwood, if we could go to page 52 in the same document, please, line 29.

BY THE CHAIR:

Q. There's a reference there to:

> Automated records destruction activities...such as the deletion of [Social Insurance Numbers]...

Now, I just was unclear. Is that a reference to the tool that we just spoke about? My understanding is it wasn't really an automated tool for the deletion of SINs before the cyberattack?

A. (Williams) (Inaudible due to away from microphone.)

Q. Sorry, your microphone, Mr. Williams.

A. (Williams) So maybe if you could just give me the question again; sorry.

Q. Yeah. No, I just -- I -- when I read this, it seemed to be suggesting that you had an automated records destruction tool for Social Insurance Numbers, which I didn't assume -- I didn't understand was the case, except for the new tool that was implemented that we just spoke about. And is that a reference to that tool, or is this something else?

A. (Williams) This is just identifying that there would -- when actions are taken on the system, so when the SINs were deleted from the CIS, there would be a -- as it's referred to here, an IT change management process or log identifying that it was done on the system, but there would not be a separate schedule

specifically saying this was deleted on such and such a date as part of the privacy program.

[2:00:04] **Q.** Okay. It wasn't intended to refer to a specific automated tool as much as a process that would have deleted the information.

A. (Williams) That records changes on the system, yes.

Q. In her evidence, Ms. Ralph noted that Nova Scotia Power's privacy training completion rate fell to 79 percent in 2025, and suggested that after an event like Nova Scotia Power experienced best practice would suggest more focus on training completion.

I wasn't sure I saw a specific response to that in the rebuttal evidence that we have been looking at here. What is the company's view of that?

A. (Williams) So I think we've attempted to be fairly clear around kind of what our position is and what our stance is coming out of that, and as it relates to training. I appreciate Ms. Ralph's view

and her opinion on that, but I think again what she, in fairness to her, would not have fully appreciated was how dramatic the impact was on the operations of the business.

So things like that training, that -- I think there needs to be understanding. On the day of this incident, really what we were left with was the ability to communicate with each other, and nothing else because as I said, we didn't have access to SharePoint, we didn't have access to nearly all of our systems.

So there's just a certain reality that needs to be acknowledged when you're looking at what that completion rate is in the face of, and then in the response, or the immediate period after the incident.

Q. Okay. And Mr. Williams, you said yesterday ---

A. (Williams) Ms. MacDonald was just reminding me to mention that, obviously that completion rate is back up to 100 percent.

Q. Great.

Mr. Williams, you said yesterday, and I'm paraphrasing a little bit here, and I could pull up the transcript if you like, but something to the effect that significant -- a significant culture shift in how important cybersecurity privacy is sort of invested in the utility after the -- after an incident like this. Do you recall that or that sentiment?

A. (Williams) I do. I don't think we need to pull up the transcript.

Q. Okay.

THE CHAIR: Mr. Norwood, if you could go to Exhibit N-11, please, and go to page 19 on the PDF, please.

BY THE CHAIR:

Q. I'm looking at the table that Board Member Melanson looked at earlier today.

A moment ago, you talked about the impact of your -- on your systems immediately after the cyber event. And in this chart of three years of sort of

phishing failure rates, it's not applicable in May and June of 2025, which I assume relates to just the possibility of actually conducting an exercise like that at that point in time?

A. (Williams) That's right, sir. I mean, I -- impossibility is a strong word, but impractability for sure, yes.

Q. Okay. And Mr. Melanson focused on that September 9.6 number. And I know you've addressed that, and in some detail with him. I do have some questions I want to follow up on with that.

But first, can you give me an understanding of what the phishing program entails at a very high level? I'm not looking for anything that would be confidential. Let me start with you've got about 2,500 full-time equivalent employees?

A. (Williams) Yes.

Q. And so how many employees in any given month might be receiving a phishing test?

A. (Williams) That would be everyone, sir, that has access to a computer. So everyone with a computer.

Q. Okay. All 2,500 employees that have access would get the test on a -- every month?

A. (Williams) Yes.

Q. Okay. And in light of that, that's, you know almost one in ten people at the company failed that particular phishing test in September, only a few months after the cyberattack, that does seem a little bit concerning and I know the response to Board Member Melanson's questions were that that was discussed at the senior management or the executive team. I can't remember which one it was.

Other than discussing it, were there specific actions that came out of that discussion to address that particular result?

A. (Williams) I think, sir, maybe some context on that discussion with senior leadership.

So those are quarterly meetings that happen with all director level and above positions within the company. And so there was a -- if I'm recalling correctly, there was a specific segment of that meeting that was dedicated to this where the statistics were reviewed and discussions were had about the emphasis that needed to be put on this and filtered down within the Company.

Obviously, we've discussed already the training that does exist and the remedial training. So every one of these employees that would have fallen victim to the phishing -- the phishing testing -- would have had remedial training. It was generally coming out of this period, following up on that month in September where the initial or the additional step was taken to impose the financial repercussions on employees. And that's what we discussed previously, where you are -- if you do fail two phishing tests, then you have that financial repercussion imposed on you. So that was the additional step that was taken to ensure that not only is the training occurring

and the message and the culture shift, but that there is a financial incentive or disincentive, depending on your perspective, I suppose.

Q. So that change was a result of those specific numbers being reviewed at that meeting?

A. (Williams) Well, it's impossible to look at any of it in isolation. That change was something that came out of what we just went through, but certainly recognizing what happened with that month in September. That change is something that flowed from the general discussion, yes.

Q. Nova Scotia Power has approximately 490,000 residential customers, subject to check?

A. (Williams) Subject to check, yes, that's approximately right.

Q. And you sent letters to approximately 375,000 of those? I think there was the first tranche of 277,000 and then the 97,000 in October?

A. (Williams) Yes.

Q. So that's about 76-77 percent of customers got a letter?

A. (Williams) I'll take your math, subject to check, yes, sir.

Q. You should never take my math. We'll go with that.

So anyway, whatever the exact percentage might have been, there was some percentage of the residential customer population that didn't get a letter, and I'm wondering if you could kind of explain what characteristics these customers had that resulted in them managing to not have personal information impacted by the data breach?

A. (Williams) Yes, sir, it would have been in -- and I'll ask anyone here to jump in as well, but it really would have been about timing and about new customers since 2021 for the most part. It's because of that cut over.

Q. Thank you. And so Nova Scotia Power would have known -- or I guess I should ask -- did Nova Scotia Power know, when it was sending out that initial batch of letters in May, that former customers who would also have been in that copy of that CIS data would have been impacted?

[2:10:57] **A.** (Williams) I think -- I mean, that was very early, obviously, but I think just the general nature of what we would have been dealing with, we would have had a sense or idea that there was likely at the very least a sense or an idea that there was likely former customers' information included in there, but for the same reason that direct notices were not sent to former customers, they wouldn't have been sent at that time either because we wouldn't have known -- we wouldn't have had current contact information for them.

Q. So it would make sense to me that you discovered this copy of this file in the Data Lake that was impacted and you went about specifically

identifying named customers to send letters to, distinguishing even between those as to who would get a Social Insurance Number version and who would not.

My question would be you also have named former customers at that point in time in your possession as a result of that exercise from the data from 1997 to 2001?

A. (Williams) So my only hesitation, sir, is I don't -- I can't speak specifically to what records within -- with what was being reviewed at the time would have had those former customers included in them. It's all part of that Data Lake cut, but as Ms. MacDonald indicated, it's a complex mis of files, and so I would assume, just like you are, that there would have been some former customers within that, but again, those would have been names and contact information that are historical in nature.

Q. No, that's fair. That's fair. But you were able to look through that data and pull up

277,000 specific names of customers. I'm assuming it wasn't by some random stroke of luck that all those names just happened to be current customers? You did identify former customers, but you had no means of contacting them?

A. (Williams) I would assume that's the case, yes.

Q. And this may have been answered. Ms. MacDonald, you may have answered it. I may just have not understood or been confused, but the ability to distinguish between customers in terms of the Social Insurance Number impact versus no Social Insurance Number impact, was that the case that right at the outset you were able to, when you were pulling the customer names out of it, you were also able to associate SINs with those names right out of the gate?

A. (MacDonald) Yes, that's my understanding as well.

THE CHAIR: Sorry, Mr. Norwood, if we could go back to Exhibit N-16? I don't know if you still

have it handy there. I think it might be the same page.

BY THE CHAIR:

Q. I know this has been fairly well covered, so it's with a little bit of trepidation that I'm going down a path again, but most of the questions, I think, focused on the paragraph that I referred to before about the types of information and the "may" sort of thing.

I wanted to focus a couple of questions on the paragraph that leads into that, if I could. So that paragraph says:

> While the investigation remains ongoing, we have determined that on or around March 19, certain customer information stored on the impacted servers was accessed and later taken by an unauthorized third party.

So would you agree with me that a reader generally reviewing that particular sentence would take from that that some information on a server was accessed and taken, but by use of the terms, "Certain customer information," it's a little bit equivocal in

terms of the information -- not all the information on the servers may have been taken?

A. (Williams) Yes, by using the word "certain" you would imply that potentially not all of the data, and I think then we're back to one of those discussions we had a few times yesterday, which is we're still not -- we still cannot be certain as to what was or was not taken for each individual customer.

Q. Right. And in terms of this notice, the next sentence goes on to say, "Your personal information was stored on the impacted servers."

So a person getting this letter is being told their information was on a server, but they are left to some degree of uncertainty in terms of whether their information was impacted. That would be the normal interpretation of that paragraph?

A. (Williams) And I think it would be the intentional interpretation of that paragraph, and it goes back to the boxes were touched, but we don't know

what from the boxes was taken.

Q. Right. You understand, though, how that might raise questions in a customer's mind in terms of the level of uncertainty and seeing something like this and wanting to get certainty?

A. (Williams) I absolutely -- as a customer myself, sir, I understand that. It's a concern we, as I said, acknowledge, appreciate and understand. There's a certain reality that we're dealing with, and it goes back to that which I just said, which is we can't definitively say what would have or what was or was not taken. So to say anything other than what was said would have been misleading.

Q. And so what was the point of sending this letter to customers to advise them that there may have been an impact on them?

A. (Williams) Well, the point was to fulfil our obligations under PIPEDA which require us to provide this type of notification.

Q. And in terms of the communication to customers, why wouldn't you have taken, as suggested by Ms. Ralph, I think, to tell customers that customer information was impacted and perhaps they should assume that anything that they provided to you was impacted as well? Do you think an approach like that would have alleviated some uncertainty? They would have some sense of what information they provided you?

A. (Williams) Not those exact words, but I do believe that's the intention of the letter, and when you read the paragraph at the bottom of the screen here:

> While we have no evidence of misuse of your personal information, as a precautionary measure arrangements have been made.

So I think that is the intent is to ensure people are made aware of the potential or taking the appropriate precautions, assuming that -- assuming effectively the worst-case scenario.

And maybe, sir, I'll just add on that

to kind of provide a bit more context. So when you -- that measure was taken and the action was not just a letter but the offering, obviously, of TransUnion, and within TransUnion, within that service, back to the discussion I had with Mr. Melanson, when you go in to register for that service, even if you're in a scenario where -- let's say just an email address had been disclosed, by virtue of that service, you have available to you to enter all of your personal information if you elect to, or none of it. So, you know, the service itself allowed for the most cautionary approach allowed for customers to protect all information. So it really was advancing that cautionary approach or the worst-case scenario approach that I think you're hinting at.

[2:20:09] **Q.** Thank you.

Is it Sejda? Is that how you pronounce that?

A. (Williams) Yes, that's my understanding as well, assuming I have it right.

Q. And that was the company that you retained to assist you in setting up your portal for the former customers that you weren't able to contact to be able to connect with you to register for the TransUnion service?

A. (Lanteigne) That's correct. It's an organization that works with external -- including TransUnion, so it was recommended to work with them to set this service up.

Q. And when did you retain them?

A. (Lanteigne) I would have to get the exact date, but it would have been in the weeks leading up to the June 25th date where that tool was launched online.

Q. Okay. So sometime early June?

A. (Lanteigne) I'd have to check exactly, but yeah, I believe it was around there, yeah.

Q. I have a few questions relating to the seasonal logic model. I know that ground has been

well covered as well, so I'll try again not to be overly repetitive.

My understanding is that by default, the system is set up so that it's got the two six-month periods, the warm period and the cold period, and the cold period goes from November 1st to April 30th?

A. (Lanteigne) You are correct, two periods, warm and cold.

Q. And what period is used on a bill is actually determined by the billing date, if I followed all the other information. So if you had a billing period for a residential customer from September the 1st to November the 1st and they got a bill on November the 2nd, all of those days in September and October would have been treated as cold days?

A. (Lanteigne) Your understanding is correct.

Q. And so I guess by design, the model itself would tend to overestimate consumption in the

first part of a cold season and underestimate consumption in the peak part of the cold season?

A. (Lanteigne) That definitely could be something that would occur for customers who, for example, heat their homes with electricity in the winter. For other customers who have consistent usage throughout the year or don't heat with electricity but do have air conditioning, it could be the other way, but yes, you have a good understanding of how that works.

Q. And there's bills that were provided in -- random bills that were provided, real bills with anonymized information on them to customers, I guess, that both showed, I think you'll agree, higher billed consumption in the November 2025 bill compared to the November 2024 bill. And in some cases or in both cases, it was not immaterial either. I think in one case it was more than double and the other, it was 40 percent higher?

A. (Lanteigne) I would have to check the evidence, but I'll take your word for it, yeah.

Q. It wouldn't surprise you?

A. (Lanteigne) Yeah, no, again, we've talked about there were some cases where, yes, we did see an increase in estimates in the month of November.

Q. And that would be particularly the case for anyone who heated with electrical?

A. (Lanteigne) Not necessarily, but yes, there could be a higher degree, someone who has a higher cold season usage could have experienced the higher estimate being in November, yes.

Q. Well, they would have.

A. (Lanteigne) Right, right.

Q. Yeah. And so recognizing this, your communications in early November, mid-November, began to turn to emphasize flexible payment options consisting of equal billing, pay what you can and photo reads?

A. (Lanteigne) We didn't really continue with that communication, I would say. One of the things that we, right from the resumption of billing in

June, when we started again, we immediately focused on, you know, the promotion of equal billing. Our support of customers who need help with payment plans on arrears balances, that's something that we've actually leveraged even prior to the cyberattack, trying to help customers find a solution.

So those messages were already out there, but yes, in November we were continuing to promote them and we have also continued, especially working through the winter months. As the meter reconnection occurred and the reconciliations occurred, we want to be very supportive of our customers to try to help them if they need that support to pay their balances off.

Q. Okay. And one of the things that you did was you reverted the model to the warm period billing on November the 21st, I think it was. So you turned that seasonal logic back to, I'll call it, warm mode.

And so you have that capability.

That's not a reprogramming thing?

A. (Lanteigne) That's correct.

So it's not -- it's not programming. It's something that in the days leading up to the change, you know, we spent some time testing it, but we do have the ability to make that adjustment.

So as you mentioned, and as we've shared previously, we did make that adjustment at that time, yes.

Q. When did you revert back to cold season?

A. (Lanteigne) It would have been, I believe, like, the second day of January. It was around then.

Q. So the customers who heat with electric heat all through December would have gotten a warm estimate for that?

A. (Lanteigne) Any customer who would have received an estimated bill would have been

following that logic, yes. It wasn't -- we weren't able to segment it by an individual customer type. We didn't have that information.

Q. Okay. And so there's a higher likelihood, then, that in December for those types of customers with estimated bills, their bills could have been underestimated?

A. (Lanteigne) That is definitely a -- yes, there would be a higher likelihood. I would agree with your statement.

Q. Nova Scotia Power, I think, was aware of the limitations of the seasonal logic model even before the cyber incident? Is that fair?

A. (Lanteigne) I think we would have understood, you know, that, as we've talked about over the -- and from a variety of angles in this proceeding that we knew that it was a legacy CIS system. We have known that -- it's something that Nova Scotia Power is looking to replace, but understanding this specific issue that we've

been talking about over the last several minutes with regards to the shoulder season issue, it was not something that -- you know, we had the awareness to make a change in advance of November 1st, I guess, if you think about it that way.

Q. You couldn't have? You weren't aware of that?

A. (Lanteigne) We could have, but we weren't aware of the impact that it would have until we actually, you know, understood and heard the feedback from our customers.

Q. In part of the rebuttal evidence -- and I could pull it up if you like, but I just -- you'll be familiar with it. There's a comment made that the CIS system, that seasonal logic, was, as they quote, "Overwhelmed by the unprecedented volume and duration of the billing disruption"; you're familiar with that?

A. (Lanteigne) It does sound familiar, yeah. I'll take your word for it. Yeah.

THE CHAIR: If you want to take a look for context, Mr. Norwood, it's N-17, page 37, line 27.

MR. LANTEIGNE: Yeah, I can see it.

BY THE CHAIR:

Q. And I just wanted to parse that out a little bit in terms of the -- how it would become overwhelmed by the unprecedented volume.

I appreciate that it was being used for a lot of customers, but as I understand it, the model was doing it -- exactly what it was designed to do. There was nothing that was breaking it because of the increased volume.

A. (Lanteigne) You are correct. The system was working.

You know, this comment here, just to add some additional context to it, the process to issue bills, obviously, is dependent on our Customer Information System, but it's also dependent on the teams that actually work to help get -- issue bills. So the volume of

estimated bills that we had created a significant increase in the workload for our billing team that helps issue bills.

So you know, combined with our ongoing support of customer concerns and helping manage to do that, to have to estimate bills for such an extended period of time, the volume of bills that were being estimated, that created more work to get the bills out the door. That volume just put pressure on us.

So you are correct. The system was working. The system was issuing bills. But it's other factors beyond CIS that were intended to be outlined in this comment.

[2:30:25] **Q.** Okay. And in terms of "Overwhelmed by the duration of the billing disruption," would it make sense that because the model uses a six-month average that, actually, as your billing disruption period approaches six months, say, in a winter period it actually would become more accurate?

A. (Lanteigne) So you're saying, if I have it right, if we estimated bills for the entire winter, would it all normalize at the end of the winter?

Q. Essentially.

A. (Lanteigne) Essentially, yes.

Q. To what extent do you feel or think that the widely publicized concerns about Nova Scotia Power's overestimation of bills, the availability of these flexible options, the potential for higher consumption winter users to have under-estimated bills -- to what extent do you think that all contributed to higher level of arrears for customers once actual meter readings became more regular?

A. (Lanteigne) It's a very good question, and there's obviously a lot of elements that can contribute to customers in arrears.

Interestingly enough, we saw the volume of customers in arrears begin to increase immediately after -- like, in June of 2025 when we resumed

billing, so we have seen that level increase right since then, and I think it actually peaked around that time.

I mean, it still is higher than we have typically seen, and I know we have commented on that publicly in different hearings.

So from my perspective, you know, right off the bat we made the decision as an organization, which I still believe is the right one, and that was not charging interest on overdue amounts, not disconnecting any customer who couldn't pay their bill. But as we were estimating bills and we were being very flexible with our customers, the other side of that meant that we didn't have the same collection activity.

So we'd be sending follow-ups. We wouldn't be following our -- you know, our regulated collection approach to engage with customers.

So that would have definitely been a factor, just the change in our management of it which, again, was really right from when the incident began.

And then we do know that heading into the winter months, it's not unique to this period of time. We do typically actually see customers in arrears increase a little bit throughout the winter months.

Again, Nova Scotia Power, winter peaking utility, that's when the most energy is consumed in the province. So we see the arrears rates typically increase and then come down as the summer.

That would have been a contributing factor.

And absolutely. I guess the point you were making as well; if a customer did have a large balance that they were not expecting, that could contribute to that as well.

But I just wanted to put some context around it because there's some other elements that we began seeing right away. There's some seasonal elements in there. And then yes, there's also this potential component, too.

Q. For your equal billing plans, am I correct that you do adjustments to those twice a year?

A. (Lanteigne) That's correct. Typically, yes.

Q. And have you noticed, in terms of the more recent round of adjustments after, you know, say January, February 2026 when more regular readings were taking place, that there was an unusual kind of degree of variance in equal billings -- equal billing plan amounts?

A. (Lanteigne) So just to actually add some context around this, I think it's an important point.

We made the decision and shared with our customers in January that we weren't actually going to be adjusting the equal billing at that time. We actually maintain them at the same level. And the reason for that was, is even though the meter reconnection had happened it hadn't been complete yet; that was completed on March the 31st. So we would not have been able to make a full

determination of what the actual usage was to adjust the payment.

So we kept the payments the same. We supported any customers who, you know, called us up to report, "You know, I put in heat pumps. I'd love to have an understanding of what my payment would look like." So we would help any customer in that regard. We'd obviously allow any customer to leave equal billing if they wanted to as well. And then we actually made the adjustments in July.

So normally we would make adjustments at mid-year. So with data available after the meter reconnection was completed on March 31st, we reassessed those accounts and made the adjustments in July.

So there's always more adjustments that occur at the annual reset than would happen in the mid-year reset, typically, putting the cyberattack aside, but this month of July, while I don't have the specifics, I do know that it was about a third of customers that did

see an increase, and the majority of customers stayed the same. And there were a few customers that actually did see a decrease of their usage profile change.

Just recognizing we hadn't made those changes in about, again, 18 months, since before the cyber incident, we actually took a look at the largest changes, and we made phone calls to those customers just to inform them of the change that was occurring. And while, you know, obviously having to inform a customer if their payment's going up, you know, we did address any concerns in the moment, but the general consensus was they were veery appreciative of the fact that we took the step to reach out so we could talk it through with them.

Q. So the third of those customers that had increases as a result of the adjustment, would that be typical, a typical volume of customers who would see an upward adjustment?

A. (Lanteigne) Yeah, I think it's fairly similar. I mean, we do know that the equal billing

payment is set at multiple points in time, and then obviously if there are changes to either the rates or any of the adjustments that can occur, it can cause increases.

So also electrification in the province, you know, is driving more people to, you know, switch from fossil fuels to electric heat, so we see usage profile changes that typically drives increase. So you know, I wouldn't say that beyond the factors that you would expect to drive the increase that it was significantly different.

Q. Sure. And in terms of the magnitude of the changes based on the recent adjustments, any difference than what you would typically see?

A. (Lanteigne) I think just because it was a year-and-a-half rather than a typical year with a mid-year check that would normally occur, the amounts were slightly more than we typically would have seen, but again, it wasn't -- it was not dramatic, if you will. So -- but yeah, it was a process that we have completed

working through.

THE CHAIR: Mr. Norwood, if you could turn to page -- is this N-17? In N-17, page 36.

BY THE CHAIR:

Q. Looking at line 6, Mr. Lanteigne:

> Photo meter reads became available again on November 21[st], 2025 as soon as operational processes were established to support their use.

I had understood your earlier comments to be that yes, this portal was open on November the 21st to do that, but before then you were still able to use meter reads. It's just the language here, "Became available again" seems to suggest there was a period that it wasn't available.

A. (Lanteigne) Thanks. Just rereading the wording and clarifying. And if the words are misleading that wasn't our intention.

But to clarify, you know, what we would intend to say is that, yes, you could get that information on our website at this date that's listed

here, November 21st, but as I mentioned earlier, we were receiving photo reads in the months leading up to that as well. Instead of having a website tool that was brought online on November 21st, we would have had the ability to just talk to a customer and accept that read and then take the information and adjust bills.

We weren't able to handle, like, the volume of them, but we leveraged them in situations where it was helpful to resolve a call that came into our Customer Care Centre.

[2:40:02] **Q.** Okay. But in -- sorry. Go ahead.

A. (Lanteigne) I was just going to say, so the wording again, you know, I do believe it had been something that had been on our website previously, but that could be what it refers to. But really, what I've clarified here is that the online tool became available. We were accepting them through conversations in our Customer Care Centre prior to that, to clarify, is

what we were doing.

Q. You didn't have an online tool, though, for uploading photo reads before this?

A. (Lanteigne) Not to my knowledge if there was one in years past, but we did not have one between when we resumed billing on November 21st, that's correct.

THE CHAIR: Mr. Norwood, could you go to -- I'm looking for Update Number 5. And if you could go to page 19. And I'm looking for, down further on the page, the last sub-bullet under number 2(a) there.

BY THE CHAIR:

Q. And the last sentence in that bullet says, "Nova Scotia Power recognizes the drawbacks of the current presentation..." -- on its bills we're talking about there:

> ...including the estimation of bills and will aim to address this functionality as part of the CIS modernization initiative.

And I just want to understand what it

is that Nova Scotia Power recognizes are the drawbacks.

A. (Lanteigne) Perhaps I can give just two examples that help illustrate it.

So the first is it's a -- perhaps not presented in the energy charges, but on our bills there's typically a line item, yeah, I think it's near the bottom of the first page, that it mentions that interest on overdue amounts is 1.5 percent a month up to 19.56 percent per annum. We -- to remove that from our bill and actually indicate to customers that late fees were not being charged, it actually took weeks of programming and testing to just change those words.

So again, it helps illustrate what we mean here, and then also some of the other conversations we've had are on the complexity of the system. So that's the first example that I'll provide.

The second one is one that -- it came up a lot in the fall, for example, when if we had estimated a bill and then we had a true read come in on

the following bill -- and I'm going to try to describe this. I've actually presented this to people to show them the bill and explain it. It's a little easier when you can see it.

But what happens, basically, is you see an entry for the meter read, which is the usage for the period of time. And I'll take an example of had one estimate for two months and I have a four-month read between reads. So the information would come in. You'd see your four months of base charges, you would see your four months of energy charges based on that meter read. That part is okay.

But the -- what ends up happening, then, is the estimated portion of that bill is removed, and when the estimated portion is removed, you can see the amount coming out. But if you take and you look at it, and you actually did the math, you wouldn't be able to understand how you got to the math, and the reason why is the base charge and the energy charge is lumped together,

and it all comes out at the same time.

So the math works. We have helped walk customers through the math numerous times to demonstrate it to them, but we did not have the ability to change it on the bill.

So we recognized that that was a source of confusion, and we filmed videos and we tried to get material out in bill inserts to help customers understand these limitations of our system. But that's just two examples of how when things need to happen, we would like additional flexibility to make changes to the bills and make items on the bill easier for our customers to understand that. And I really hope I've explained the estimated bill one right because it's much easier when there's a visual, but hopefully -- if there's any questions I'd be happy to answer on that explanation.

Q. Okay. I think I got it well enough to understand the point that you were making. So I take it that high on your wish list for the new CIS is a

more nimble module, if you want to call it that, to be able to design and redesign bills on the fly to have ---

A. (Lanteigne) You have much more succinctly described what I just explained, yes. Thank you.

THE CHAIR: And if we could just go to the next page, Mr. Norwood.

BY THE CHAIR:

Q. The first bullet at the top of the page refers to billing inserts, four billing inserts to communicate information about the incidents' impact on billing the need for estimated bills and the options and supports that we've discussed already.

I'm not sure that those billing inserts were put into evidence at this point. I know some communications were; I don't know if those were ones.

A. (Lanteigne) We're not certain if they have been entered. What I can say, as well, is the number would be -- you know, actually would be larger than

four. I think we're continually providing bill inserts. And one of the pieces -- we've heard feedback that, you know, we potentially hadn't included bill inserts; we've had them right since we resumed billing in June. So we'd be happy to take an undertaking to actually provide the bill inserts so that the Board could review them.

Q. Yeah. And would they all have been the same or would they be modified over time?

A. (Lanteigne) The inserts that were put into customer bills have evolved so, yes, every bill would typically have something with it, but we've evolved. It's just based on the situation and for some of the items that we've discussed earlier, just the evolving, the situation itself. You know, if we've seen feedback from our customers, we've tried to include it. We've talked about photo reads so we would have one that has that listed on it. And we'd be happy to share those as an undertaking.

Q. If you would, that would be

appreciated. And if you could do it in a way -- I don't know if there would be dates on the billing inserts themselves, but if you could date the vintage of them so I know how the various iterations changed over time.

A. (Lanteigne) We'd be happy to that, yes.

Q. Thank you. So that will be Undertaking U-17.

UNDERTAKING U-17 - To provide the billing inserts, with the dates they were provided to customers

THE CHAIR: Mr. Norwood, if we could go back to Exhibit N-17, please, page 34, line 13.

BY THE CHAIR:

Q. So this is a critique of Ms. Ralph's evidence and there's a reference to an instance in Saskatchewan:

> ...where the Information and Privacy Commissioner recommended that credit monitoring be provided for a minimum of ten years in response to a privacy breach...

And that sentence goes on to say:

> ...however, the breach compromised personal health information such as names, addresses, dates of birth, height, weight, telephone number, email addresses, dates, location of services, health diagnosis/condition, [medical]/prescriptions, medical record number, patient numbers, health insurance/subscriber number...

Et cetera, et cetera. And that seemed to be some sort of a justification for, as I read it, why 10 years would be more appropriate in that case as opposed to this case. Is that a fair understanding of the purpose of that information in Nova Scotia Power's evidence?

A. (Williams) I think it's just adding context there about that decision and noting that that's the distinction between the types of information that are at issue here as compared to the ---

Q. Right. And this was in the context of credit monitoring service?

A. (Williams) Well, it's in the context as I would understand it. And, again, I'm not

overly familiar with the Saskatchewan decision in detail, but I would understand it as the same type of service that is offered -- has been offered by Nova Scotia Power with TransUnion. And that is in part credit monitoring, but it is also identity theft protection. So it's more than just credit monitoring. I think it goes to the point, I suppose, that the more personal information you're disclosing, perhaps the higher risk you are for identity theft.

[2:50:12] **Q.** Sure. But in terms of credit monitoring and identity theft, wouldn't a Social Insurance Number be more significant than a prescription? You've got a series of health-related datas, and I guess I'm having difficulty understanding why that would justify a longer period of credit monitoring as opposed to a Social Insurance Number.

A. (Williams) And I don't know for sure that the Saskatchewan decision didn't involve an instance where SINs were disclosed. It also included

health information and health insurance number, patient numbers; like, it's all sensitive personal information.

Q. Maybe I'm reading too much into it, but it seemed to me that this was presented by Nova Scotia Power as the distinguishing reason why there might be a longer period in the case of Saskatchewan and not here; is that correct?

A. (Williams) I think again, sir, it's just trying to provide more context around the decision. I don't know that we drew any conclusions as to what was appropriate in those circumstances or not.

Q. And you're not asking me to?

A. (Williams) I am not.

THE CHAIR: Mr. Norwood, if we could pull up Update 11 now, please, and go to page 11.

BY THE CHAIR:

Q. And we can't see the top of the page; it's cut off a little bit there, but you'd recognize that as information relating to the payment by Nova Scotia

Power of outstanding bills?

A. (Williams) Yes, sir.

Q. Okay. And this information was presented in various updates over time, and the chart has expanded more in the -- in Version 11, I guess, so it's a little bigger than it was when it started out.

I'm just wondering how I am supposed to read this. And so I've got a few questions related to that. So question one is, does each column represent the outstanding bills to be paid by Nova Scotia on a specific day or over a specific time period?

A. (Williams) My understanding, sir, it would be as of the specific day that's at the top in the yellow highlighting.

Q. Okay. And the April 2025 pre-cyber one doesn't have a specific day, but I'm assuming again that is a specific day before the cyber incident?

A. (Williams) Yes. I don't know if it's April 24th or a random day in April, maybe the middle

of the month. I'm not -- as you indicated, we're going back eleven iterations of this; I don't recall what the originating data related to.

Q. And would the day have been chosen because it would have been a typical snapshot of any given day in terms of the payable situation for Nova Scotia Power?

A. (Williams) That would be my assumption as that's certainly my understanding of the intention of the exercise.

Q. Okay. Now, in the rows below the top line, you've got those other yellow rows that have reasons 36 to 60 days, 61 to 90 days and 90-plus days; do you see those?

A. (Williams) I do.

Q. What do those particular rows, or the sub-rows under them, what am I supposed to take from that?

A. (Williams) Sorry; is that in

relation to the Administrator of Procurement?

Q. Yes.

A. (Williams) So then you'd go own to the legend, if you will, at the bottom of the page, and that has a (inaudible due to mumbling) of what would be the rationale or the reasons contained within those sub-rows or sub-headings.

Q. Okay. And there's no ---

THE CHAIR: If we can go back, Mr. Norwood.

BY THE CHAIR:

Q. There's no kind of hold reasons for the 0 to 35 day range. Is there a particular reason for that?

A. (Williams) I think that would just be because it's -- that -- that's a typical range and there's nothing -- there's no reason as to why it would be in the 0 to 35. That's a typical pay period.

Q. Okay. All right. So that was

sort of the normal course, no particular reason for having it extend beyond the normal?

A. (Williams) That would be my understanding, sir, yes.

Q. Okay. Now, if I look at the hold reasons 90 plus days at row underneath there, and I'm looking at the bold numbers at the bottom line for the pre-cyber, I've got about 148. Do you see that?

A. (Williams) I do, yes.

Q. If I go all the way across to the most recent version in August 4th, 2026, which is 744 in the 90 plus days, that's materially higher than it was in the pre-cyber number?

A. (Williams) It is. It's ---

Q. Mic.

A. (Williams) I'm off.

It is. The total invoices in that month are also higher. So there would be a proportional impact as well.

Q. Right, but there have been -- there has been no point since the cyber incident when it's been even close than the 90 days to the same number that appears on the pre-cyber number?

A. (Williams) Yes. And I think part of that reason is you'll see the kind of trend downwards until you get to about the middle of, or two-thirds the way across the page, moving to the left, and then you get to a point where we were standing up our new financial systems. And so there were some learning curves associated with that.

Q. So -- okay. Fair. Regardless of the reason, cyber or new accounting system, this data does not show that you have recovered in terms of a plus 90 category of invoices, that you've gotten them down to a level that's pre-cyber?

A. (Williams) Well, I haven't done the math on all of it, sir, but certainly when you look at the total invoice, I mean the April invoice is 1690, when

you look at the middle of the page, the March invoice is 3700, you're over twice as many total invoices. So the number may still be higher even on that proportional basis.

But I do believe that things were trending in the right direction, certainly, particularly when you account for the increased amount of invoices that are in the system. And then, like I said, there was the implementation of the new financial system.

Q. And in terms of increased amount of invoices on the system, is there something that's happened that's caused Nova Scotia Power to suddenly get more invoices?

A. (Williams) Nothing that I'm aware of, sir. I suppose there's likely some seasonality that's at play there as well. You'll see in the July that the number is down considerably at 1400, and that's similar to where it was in April. But nothing that I'm aware of that would provide you an explanation.

Q. Okay. In going up the chart there, the 61 to 91 days, we could have a similar discussion in terms of the pre-cyber levels, that the numbers there are not showing that the outstanding invoices that are in the 61 to 90-day range have returned back to pre-cyber numbers?

A. (Williams) Yeah, I would suggest it's a very similar discussion to what we just had.

Q. Same for the 36 to 60-day?

A. (Williams) Well, I think July would be a bit of an outlier.

Q. It would be. It would also be a bit of an outlier for only having 16 in the 0 to 35-day range, as opposed to the 1306 in the pre-cyber range. Any reason why there's only 13 invoices on that particular day outstanding in that range? Sorry, 16?

A. (Williams) I -- you're really testing me on the numbers, sir. I don't have an explanation as to why that would be the case. We can --

we're certainly happy to enquire further if it would be helpful, but I don't know what the explanation would be at this point.

Q. Okay. And in terms of the overall total invoices across all bands, all times from 0 to 91 plus, sorry, 90 plus days, aside from that issue that whatever's going on in July, you'd agree with me that there's no real indication that those invoices have returned to pre-cyber levels?

[3:00:04] **A.** (Williams) Sorry, on the 60 to 90 ---

Q. Oh.

A. (Williams) --- total?

Q. So to the top bands total between all days, you've got 1690 for pre-cyber in April.

A. (Williams) So that would be all invoices in the system. So I don't know that that would be indicative. The total, I don't -- I'm not sure that would be indicative of impacts of cyber or recovery from

cyber.

Q. So if I'm to take the April 2025 as sort of a typical pre-cyber outstanding number, when I look at this I'm not seeing anywhere, except with whatever might be going on in July, of indicating that there's anything that's really relatively close to pre-cyber levels in any of this data.

A. (Williams) Yeah, I guess the shortcoming of this table is that what we were asked to do and what we did was provide the April cut in time, and it goes back to the discussion we first had; it's not clear that that's necessarily representative, and maybe that's throwing off the whole discussion.

Q. Okay. Is there something else? So one of the complaints that the -- that has been made is after the cyber incident was that Nova Scotia Power wasn't paying its bills on time and a lot of its creditors were being left with cashflow problems and other issues.

This is supposed to be evidence to

demonstrate that things are okay, and that things have now returned to pre-cyber levels. I guess you're right, there's some limitations to it. Is there something else you think you can provide to demonstrate otherwise?

A. (Williams) Well, as I said, I do think, you know, working from what's on the chart, that it demonstrates a trend in the right direction to recovery, and then as I said, there was the standing up between financial systems. Certainly aware of the concerns that were raised at the time, and the ones that you're referring to. I'm not aware of current concerns to the same magnitude. So that would be a factor that's relevant to the discussion.

Q. And the new financial systems, was that needed as a result of the cyber incident?

A. (Williams) Yes.

Q. So if I accept your thesis that this is demonstrating a, you know, a good downward trend, when does Nova Scotia Power expect to be back to pre-cyber

levels in terms of invoice payments?

A. (Williams) I don't have a specific date, sir, but as referenced in the body of the report, that it's indicated that those numbers are expected to come down over the coming months as we gain operational familiarity with the new system.

Q. In terms of costs of the cyber incident, and again I'm approaching this with the same caveat that Board Member Melanson made this morning, the commitment that Nova Scotia Power made to customers not paying costs relating to the cyber incident, I think that's been canvassed. I think I understand that, you know, if but for the incurring of cyber costs there might have been an overpayment, I understand the commitment doesn't extend that far as well. That's correct?

A. (Williams) Sorry, sir. When you refer to an overpayment are you ---

Q. So overearnings. So if ---

A. (Williams) Oh.

Q. Sorry, sorry, I misspoke. If customers, but for the incurring of expenses relating to the cyberattack, would have been in the zone where they would have been eligible for overearnings, I understand that to not be part of Nova Scotia Power's commitment based on testimony we heard yesterday?

A. (Williams) Yeah. So Nova Scotia Power's commitment -- I just want to be clear on this point, I guess, that the commitment is that customers will not pay for the costs of restoration which are expected as is included in the evidence generally being concluded by the end of this year, which would mean they're not in customer -- not included in rates.

Your question then being if we were in a scenario where Nova Scotia Power had earned over the 9.25 and 40 band, then would money be returned to customers. And in my mind, sir, that's a hypothetical that I don't know that I'm in a position to speak to.

I mean, we talked yesterday about

there being a preliminary question as to whether we're even at 9.25 and 40, and the information that is on the record would not indicate we're in that realm.

Q. For 2025.

A. (Williams) For 2025. Twenty twenty-six (2026) is obviously yet to be determined, but it -- I'm fairly certain it will be a similar discussion.

Q. But in terms of the commitment, which is what I was focusing on, the commitment shouldn't be understood as relating to that at all.

A. (Williams) No. It's the immediate costs.

Q. In terms of the costs that have been incurred, we have that confidential response to the CA IR-6 that we've referred to.

Have capital costs been incurred?

A. (Williams) Yes, there would be capital costs included in the costs that are outlined in that attachment to CA-6.

Q. They're included in the attachment?

A. (Williams) They would be -- there would be capital costs that are included in the costs itemized there, yes.

Q. Okay. So ---

A. (Williams) Yeah, what I was -- I guess in my mind went without saying, but what I probably should say is that we obviously don't intend to apply to the Board for those costs. Those are capital costs that have been incurred by the utility and will not be sought from customers.

Q. So capital costs would typically go into rate base. You're saying you're expensing them in full 100 percent?

A. (Williams) So an example would be rebuilding the AMI platform. So those were capital costs that were incurred that customers have paid for once. We would not expect them to pay again.

Q. And what about other hardware, tablets, servers, all of that stuff? Was there capital costs incurred in replacing assets of that nature?

A. (Williams) It'd be the same discussion, sir.

Q. So those won't find their way into rate base?

A. (Williams) The replacement costs -- and there would be rate-based costs for the original.

Q. The original.

A. (Williams) The original, yes.

Q. Okay. So the original equipment would be retired and recovered through the pools, I guess, and -- but you're not adding the new assets?

A. (Williams) That's my understanding, yes.

Q. Your understanding.

A. (Williams) Yes, sir, that's our intention.

Q. Thank you.

I had just one question following up on a question that the Small Business Advocate had asked yesterday.

You may recall that she had a line about impacts on small business class customers and whether or not they would have gotten letters and so on.

Did it make a difference in terms of their corporate status? So if they were sole proprietors, for example, would that have gotten them letters relating to personal information or not?

[3:10:33] **A.** (Williams) It would not have, sir, and even in the instance where you're speaking of, that information would have been provided for a business purpose and so would not have been considered personal information.

Q. Okay. Thank you.

Just give me a moment.

(SHORT PAUSE)

THE CHAIR: Yeah, those are my questions.

Do you have something, Mr. Deveau?

VICE CHAIR DEVEAU: Yeah. I just had one point. Sorry, I apologize.

I had asked the panel questions about the '25 financial statements. I wanted to enter that on the record.

It is sequential, so there's no interruption in sequence. I apologize to the transcribers.

But the attachment that was referred to was the management discussion and analysis. It was from Matter M12835, the 2025 financial statements, Exhibit

N-2, Attachment 3.

THE CHAIR: Thank you.

And that will be Exhibit N-23.

--- EXHIBIT NO. N-23:

Exhibit N-2, Attachment 3 from Matter M12835 - 2025 financial statements - management discussion and analysis

VICE CHAIR DEVEAU: Thank you.

THE CHAIR: Anything arising from any Board Panel questions from any of the parties?

I don't see any. Okay.

Mr. Clarke, anything by way of re-direct or arising?

MR. CLARKE: Mr. Chair, there's no re-direct.

THE CHAIR: Okay. Thank you

Did anyone have any questions for a confidential session for this panel?

Okay. I'm not seeing any, so I think that concludes your testimony. Thank you very much. Appreciate your patience over the past couple of days.

MR. WILLIAMS: Thank you very much, sir.

(WITNESS PANEL WITHDRAWS)

THE CHAIR: I've been running for a bit. It's probably good for a break, Mr. Clarke, and that will help get set up with the next witness. Is that okay?

MR. CLARKE: Yes, I agree.

THE CHAIR: Okay. So it's about quarter after 3:00 now. We'll come back at 3:30.

--- Upon recessing at 3:13 p.m.

--- Upon resuming at 3:30 p.m.

THE CHAIR: I think we're good to start.

Mr. Clarke?

MR. CLARKE: Mr. Chair, I don't see Ms. Valdetero yet on the screen.

MS. VALDETERO: I'm here. Are you guys unable to see or hear me?

MR. CLARKE: We can hear you; we can't see you.

MS. VALDETERO: Give me one second. Let me check my settings. There we go. Can you see me now?

[3:30:47] **MR. CLARKE:** Yes, we can.

MS. VALDETERO: All right. Excellent.

MR. CLARKE: Ms. Valdetero, can you please confirm you've filed evidence in this matter -- oh, I'm sorry. It's been a long day, sorry.

THE CHAIR: I'll try not to take that personally.

MR. CLARKE: No, no.

JENA VALDETERO, Solemnly affirmed:

THE CHAIR: Go ahead, Mr. Clarke.

MR. CLARKE: Thank you, Mr. Chair.

EXAMINATION ON QUALIFICATIONS BY MR. CLARKE

Q. Ms. Valdetero, can you please confirm you filed evidence in this matter which has been marked as Exhibit N-17, Attachment 1?

A. Yes, that's correct.

Q. And you provided a summary of your qualifications and experience which is marked as Exhibit N-17, Attachment 1, Appendix A?

A. Correct.

Q. And you are a practising lawyer and a Co-Chair of the U.S. Data Privacy and Cybersecurity Practice at your firm, Greenberg Traurig; is that correct?

A. That's correct.

Q. Have you appeared before the Board as a witness in the past?

A. I have not.

Q. Can you please provide a summary of your professional qualifications?

A. Sure. I am a practising attorney and a shareholder at Greenberg Traurig. As you mentioned, I co-chair the firm's U.S. Data Privacy and Cybersecurity Practice. I graduated from Georgetown University Law Center with a juris doctor law degree in 2005. I started practising as a litigator and started handling data security incident response back in 2012.

Since then, I have had a high-volume practice, advising hundreds of clients on more than 1,000 data breach investigations, including a significant number of ransomware and/or extortion matters. My role in advising clients includes leading an incident investigation, retaining vendors like the one that Nova Scotia Power retained here, including forensic investigators, document review vendors and notification vendors. I advise clients on their obligations under various data breach notification laws both in the United

States and international laws, including in Canada, like PIPEDA and other similar provincial laws.

To be clear, I am not a Canadian licensed attorney. When we are engaging on Canadian matters, we typically will partner with a local Canadian firm, although not always.

I also regularly publish articles and speak about data security issues.

Q. With respect to your opinion in this matter, what were you asked to do?

A. My review was limited to the steps taken by Nova Scotia Power after the cyberattack was identified and to the Company's communications with the customers and notification efforts.

Q. You've confirmed your pre-filed evidence. Are there any corrections to that evidence?

A. No.

Q. Are the facts on which your opinion is based true and accurate to the best of your

knowledge?

A. Yes.

Q. Are the opinions expressed in your evidence your own?

A. Yes.

Q. And you've reviewed the evidence of InterGroup and INQ Law as part of your review?

A. I have.

Q. And you've reviewed the parties' opening statements?

A. Yes.

Q. And you've heard the testimony provided throughout this hearing?

A. I have.

Q. Did any of the evidence filed or heard have any impact on the conclusions drawn in your evidence?

A. No.

MR. CLARKE: Mr. Chair, Nova Scotia

Power requests that Ms. Valdetero be accepted as an expert witness in the areas addressed in her evidence, specifically coordinating incident response activities, including incident investigations, notification obligations, adherence to relevant data breach laws and best practices.

THE CHAIR: Any questions on qualifications or objections?

She is so affirmed, Mr. Clarke.

MR. CLARKE: Thank you, Mr. Chair.

Ms. Valdetero is now available for questions.

THE CHAIR: Consumer advocate?

MR. ROBERTS: No questions. Thank you.

THE CHAIR: Small Business Advocate?

MS. MacADAM: No questions. Thank you.

THE CHAIR: Mr. MacLeod?

CROSS-EXAMINATION BY MS. AKCAKIRYAN

Q. Could we turn to Exhibit N-17, please, PDF page 85? So line 20.

Ms. Valdetero, in support of your opinion about industry practice, you rely on statistics supplied by TransUnion?

A. Correct, yes.

Q. Thank you. The data from those statistics are not reproduced in this report, though, is that right?

A. I'm not totally following your question. Do you mind rephrasing?

Q. Absolutely. So you refer to -- I believe it's at line 20, it says, "According to statistics provided to NS Power from TransUnion". Did you review those statistics?

A. I reviewed the information provided from TransUnion, and that information included statistics compiled by TransUnion for 2025 data breach,

credit monitoring offerings through TransUnion. That information stated that only six percent of companies that have hired TransUnion in 2025 to provide credit monitoring for a data security incident had utilized five years of credit monitoring.

Q. Okay. Thank you.

And because we don't have access to those statistics, can you advise us as to how many affected individuals were Canadian Armed Forces members?

A. I am not aware of that information.

Q. In preparing your opinion for Nova Scotia Power, did you assess how many affected individuals held federal security clearances in Nova Scotia?

A. I did not.

Q. Okay. So your conclusion concerning the reasonableness of the five years of monitoring does not incorporate any assessments specific

to customers holding federal security clearances and the inherent elevated consequences associated with that?

A. I was not specifically asked to opine on the offering of credit monitoring to different people in various situations where they would be distinguished from each other, no. It would not change my opinion, though.

Q. Okay. Thank you for that.

So now, can we turn to page -- PDF page 92, please? I believe line 16, you describe the myTrueIdentity service offered by Nova Scotia Power as a comprehensive package; is that correct?

A. Yes.

Q. Perfect. And we also know that Canada has two major credit bureaus, TransUnion and Equifax?

A. Yes.

Q. And lenders don't necessarily report to both bureaus; is that right?

A. That's my general understanding is that not every furnisher of information reports to every credit reporting agency.

Q. Okay. So for example, if fraudulent credit activity appeared on an individual's Equifax credit file, would that activity necessarily trigger an alert through the TransUnion Credit Monitoring Service?

A. I am not sure. My understanding is it was monitoring TransUnion alerts, but I'm not clear -- I would have to talk to TransUnion about whether there's any tracking for Equifax as well.

Q. Okay. Thank you for that.

And can we move now onto page 94, PDF page 94, line 6, please.

So you rely in your report on the fact that customers can continue to access their credit information for free after the five-year monitoring period expires. Is that correct?

A. Yes.

Q. Okay. And in your view, is accessing a credit report and having a credit report actively monitored two different services?

A. So accessing a credit report enables you to be able to review what has been queried on your report, to the extent it's reportable, and also review what credit has been opened in your name. My understanding is credit monitoring is an alerting system that would send you a communication if someone enquired about or opened a line of credit in your name.

[3:40:14] **Q.** Okay. So then would it be fair to say that active monitoring is designed to alert the consumer to specific changes?

A. Yes.

Q. Okay. But with free access to a credit report, the consumer must take the initiative to obtain and review that information periodically; is that correct?

A. That is correct, which is a best practise of consumers. Individuals should be doing that on a regular basis.

Q. Okay. And my understanding is that the myTrueIdentity service also offers Dark Web monitoring. Would the free access to credit report notify a customer of any Dark Web activity?

A. No.

Q. So free access after five years does not necessarily provide the same active monitoring as the five-year subscription.

A. It does not, but I think nobody offers credit monitoring in perpetuity following a data security incident. But it is not the same.

Q. Okay. And the future risk associated with the compromising can persist beyond five year -- a five-year period; is that correct?

A. Theoretically, exposure of that information could create a risk in the future. The more

time you get away from the source of an exposure, the less likely that it is to happen, or at least the less likely it is to happen as a result of that particular data security incident.

Unfortunately, the reality is because there are many breaches, our information has probably been exposed multiple times, and sometimes we'll have individuals who will report that they believe their information was detrimentally used because it was exposed in a particular incident, and you really can't connect that use, or that misuse of that information to a particular incident. The longer time that passes, the less likely you are to be able to do that.

Q. Okay. But would you say that you do agree that there is a future risk following a five-year period?

A. I think there is always a risk. It dissipates over time as it relates to that particular -- that particular incident.

Q. Okay. Thank you.

MS. AKCAKIRYAN: Those are all my questions.

THE CHAIR: Thank you.

Industrial Group?

MS. RUDDERHAM: No questions, Mr. Chair. Thanks.

THE CHAIR: Department of Energy?

MR. KAYTER: No questions, Mr. Chair. Thank you.

THE CHAIR: Mr. Mahody?

MR. MAHODY: Thank you, Mr. Chair.

CROSS-EXAMINATION BY MR. MAHODY

Q. Ms. Valdetero, I'm Bill Mahody. I'm counsel to the Board. I have a few questions for you based in your report.

A. Sure.

Q. Could I start under section 3 of your report, the page 4 of 32.

MR. MAHODY: And if we can scroll down. Page 4 of 32 of -- sorry, at the bottom corner, bottom right corner, 4 of 32.

MR. NORWOOD: Yeah.

MR. MAHODY: Okay.

BY MR. MAHODY:

Q. All right. It's coming on the screen now, Ms. Valdetero. It's the Information Considered. And in preparing the report, you note the items that you've considered.

And if we can turn over on to the next page, the last bullet of Information Considered is:

> Information obtained from representatives of TransUnion, [Nova Scotia] Power, [Osler's], and Emera.

Do I correctly read your background and experience, Ms. Valdetero, is normally you're retained in these matters to be fulfilling a role similar to Osler's role in this breach?

A. That's correct.

Q. Do you have any direct experience, Ms. Valdetero, in advising regulated utilities regarding the collection and storage of customers' personal information?

A. Yes.

Q. Tell me about that.

A. So I have advised a large utility and nuclear power plant company in the United States. I'm their primary outside data privacy, or only outside data privacy and security counsel for the last five years.

Q. Any other direct experience advising regulated utilities on collection and storage of

personal information?

A. Would you include a telecommunications provider as a regulated utility?

Q. Yes.

A. Okay. Then yes.

Q. All right. Tell me about that, please.

A. So I have provided external data privacy advice and counselling to a large telecommunications provider, oh gosh, probably for the past four years on data security matters, in particular, including large-scale incidents. A second outside cellular telephone company, we provide advice and counselling to them as well on data privacy and security matters.

And I apologize, for confidentiality reasons, I can't share the names of these companies. I hope that's okay.

Q. That's just fine. Can you tell

me, Ms. Valdetero, are any of those utilities that you mentioned, are they similar to Nova Scotia Power in that they're vertically integrated single providers within the jurisdiction they operate?

A. Yes. The energy company is.

Q. Okay. And I take it as part of your work, you're familiar with the term of "data minimization", Ms. Valdetero?

A. I am, but note that that was not part of the scope for which I was retained to provide expert advice in this matter.

Q. But when we're referring to best practices, it would involve the utilisation of data minimization?

A. Where are you referring to best practices; I'm sorry? Are you referring to a specific part of my report?

Q. In your qualifications today, there was reference to the best practices, and I'd like to

ask you about the use of data minimization as a best practice for the collection and storage of personal information.

MR. CLARKE: Excuse me. With all due respect, that was not part of the retainer for this expert. The retainer was in relation to responding to the cyberattack itself. We didn't ask her to look backwards in time.

THE CHAIR: Mr. Mahody?

MR. MAHODY: So Mr. Chair, I would simply point out that the scope of the qualification had to do to the matters referred to in her evidence. In her evidence, there is reference to being involved in thousands of data security incidents. I think that this practice, the minimization of data, is a factor for consideration.

MR. CLARKE: Well, she's entitled to talk about her CV, experiences and qualifications, but it's the scope of the retainer which is what's relevant,

the four corners of her opinion. Just as I wouldn't be able to ask her all kinds of opinions with respect to things that she wasn't retained on. That would be unfair, and it's not appropriate to ask her things that she hasn't considered, hasn't thought about. We didn't ask her to look at that.

(SHORT PAUSE)

[3:50:05] **THE CHAIR:** Mr. Clarke, generally I think the panel is of the view that like all expert witnesses, this expert witness is here to assist the panel in coming to an appropriate understanding and resolution of the matter before it. We think in some respects, potentially this line that Mr. Mahody is going down, may be useful in terms of providing that. We do take your point that it's not -- it may not be appropriate to ask her in terms of fresh opinions that she hadn't given thought to on entirely new matters, but at this stage we're inclined to see where it goes.

MR. CLARKE: Mr. Chair, with the

greatest of respect, I would like to identify my objection to this. If we wanted her to give an opinion with respect to other areas, we would have sought it, we would have asked for it. She hasn't considered it; she hasn't looked at the material in relation to it. These are not issues that were put to her. And to have to now respond to them on the fly is inappropriate. This idea of best practices, the best practices were in relation to what she was retained to consider, which is the steps forward from the cyberattack, not backwards.

Now she's being asked to offer opinions in relation to things she didn't consider. Yeah, I think the Board wants the best evidence. And the best evidence is not answering questions in this tunnel fashion, as far as I'm concerned.

THE CHAIR: Thank you, Mr. Clarke. We've made our ruling so we'll see where it goes.

MR. CLARKE: Thank you, Mr. Chair.

MS. VALDETERO: Can you repeat your

question?

BY MR. MAHODY:

Q. Certainly. So Ms. Valdetero, you're familiar with the term "data minimization"?

A. I am.

Q. And does that represent a good -- the good practice that personal information, when it's no longer needed to provide a service, that it's removed from a business' dataset?

A. In general, I would agree with that definition.

Q. Fair enough. And in your CV you specifically make reference to regularly publishing articles and speaking publicly about data security issues. Data minimization would be a topic that you're familiar with through those articles, publications and presentations?

A. Off the top of my head I can't think of anything specific where I've given a presentation

on data minimization, but in general I am familiar with the concept.

Q. And also in your CV, in the fourth bullet of your -- or fifth bullet of your areas of concentration, you talk about analyzing privacy and security liabilities and risks of target companies in mergers and acquisitions.

A. Yes.

Q. If a target company had stored a large trove of information that was -- or personal information that was no longer required, would that be the typo of risk that that work that you do would identify?

MR. CLARKE: Mr. Chair, I don't wish to be a nuisance, but by the same token, am I supposed to object each time one of these questions comes up? Because it's not appropriate, and I object to it.

THE CHAIR: Mr. Mahody?

MR. MAHODY: The witness is an expert, is an expert who has expressed familiarity with data

minimization and she has indicated examining risks in certain situations, and I'm simply asking whether or not data minimization is one of the risks that she would be familiar with assessing in that situation that is referenced in her CV.

MR. CLARKE: Mr. Chair, her CV is not the issue here; it's what she was asked to offer an opinion on.

THE CHAIR: To address your first point, you can object any time you want, Mr. Clarke, don't feel the need that you're beating a dead horse or whatever. If you feel you need to object, you object.

To address the more significant issue, I think, as you're aware the Board's approach historically has been fairly liberal in terms of cross-examination of expert witnesses. This is not a new thing.

I still take your point that there are limits to that, Mr. Clarke.

Mr. Mahody, could you repeat the

question that you intended to ask?

MR. MAHODY: I was going to ask Ms. Valdetero whether when she is analyzing -- when she's undertaking the work that involves the analyzing of privacy and security liabilities and risks of target companies in mergers and acquisitions, if a target company had a large trove of stored but no longer needed customer personal information, would that be a risk Ms. Valdetero would identify?

MR. CLARKE: I object to that question and it's a perfect example of a question asked in a vacuum without any context. It goes to the issue of my client's actions in this. Ms. Valdetero hasn't looked at the surrounding circumstances; it's not part of her opinion, so I object to the question.

THE CHAIR: And how far down this trail do you intend to go, Mr. Mahody?

MR. MAHODY: You've seen it; that's the whole trail. My next question will be in a completely

different area.

THE CHAIR: Yeah. Well, why don't we move on to that one then?

BY MR. MAHODY:

Q. All right. Ms. Valdetero, could I take you in your evidence to your critique of Ms. Ralph and Ms. Ralph's recommendations regarding the reasonableness of the timeframe for notifying former customers?

A. Sure. Is there a particular page you would like to direct my attention to?

Q. There is. It's at page 8 of 32, section 6. And here you're addressing the timeframe for notification to former customers. Do I take it, Ms. Valdetero, that one important factor when assessing that reasonableness is when Nova Scotia Power should have been aware that the data of former customers had been compromised?

A. One important factor is when they

were aware that data had been compromised, yes. That's one of several factors though.

Q. And when you were considering the reasonableness, we have the June 25th date being the date that the notification to former customers was made. What date were you utilizing for the start date of that period when you were trying to determine reasonableness?

A. I believe it was May 1st, but allow me to check my timeline, if you don't mind, so I'm not giving bad testimony on this point. Yes, May 1st, Nova Scotia Power determined customer personal information had been impacted and provided an update on its website to that effect.

[4:00:17] **Q.** And in relation to the notification to former customers on June 25th, 2025, it's your view that the period between May 1st to June 25th is a reasonable period?

A. Yes, particularly given the amount of resources that needed to be pulled together in

order to get everything ready to make that notification, ensure it was distributed widely, ensure credit monitoring was set up, ensure that information resources were available and were working as intended in order to avoid creating more confusion.

I laid out in the report several factors of things that had to be done before you could actually go live. And with respect to Ms. Ralph, who is obviously quite qualified in the privacy space, if you haven't spent a lot of time working on actual data security incident response, it's hard to imagine all that goes into having to put the pieces together to be able to make notifications. It's far more involved than you think. If it were as easy as, you know, kind of flipping a switch and being able to make that notification, then this timeframe would not have been reasonable, but given all that needed to happen in that timeframe, from when they first identified -- and I wasn't sure when they first identified former customers, but I was still basing it off

of May 1st, when they first identified that information may have been affected to be able to execute a strategy on this scale, this is a very reasonable timeframe.

Q. Can I take you next to addressing the second finding. I'm on page 13 of your report. And this is regarding the notification in October of the 97,000 additional customers. And I'm looking at line 12 of your report, and you say that:

> The October 31 direct mailing should be understood as a later, more individualized outreach step...

Now, I appreciate that the October 31st is later in time than May 13th, but what did you mean by a more individualized outreach step?

A. So one thing that's notable is that Nova Scotia Power, from the time it identified that personal information of customers may have been affected, was going out and making that very public. So they were -- they made a public announcement on May 1st. They were regularly updating their website with updates and

information. They were reaching out to media sources all around the province. They were deploying teams locally to help people in person, have their questions answered. They were making credit monitoring -- as of June 25th, five years of credit monitoring -- available to any Nova Scotia former or current customers. So what I'm referring to is the fact that this is not the first time that these individuals would have heard that there had been a substantial cybersecurity incident at Nova Scotia Power.

There was a consumer poll survey that was done in July, so a few months before this, and that survey revealed that 85 percent of the people surveyed knew or had some information about the security incident. So obviously the steps that had been taken to raise public awareness had been quite effective several months before.

MR. MAHODY: Thank you, Ms. Valdetero. Those are my questions, Mr. Chair.

THE CHAIR: Mr. Melanson?

QUESTIONS FROM MEMBER MELANSON

Q. I just have a few questions. The first one, same exhibit at PDF page 7, and lines 13 to 16. And this relates to a discussion about the scale of the attack. It says:

> NS Power's response to the Incident should be assessed in the context of a large-scale ransomware event involving extensive data exfiltration, severe operational disruption by the Company and forensic uncertainty common for large-scale ransomware incidents.

And I'm just wondering whether you, without divulging any solicitor-client information, whether you had personal experience with respect to ransomware attacks of this size?

A. Substantial experience. I would say several hundred matters involving large-scale ransomware attacks.

It might be helpful to provide a little bit of history about how data breaches have evolved, because I do think it's helpful to the panel --

to the Board.

So when I first started doing incident response 14 years ago, it was not very common, right? We'd have one or two matters a month. It was a lot of credit card theft, at least in the United States because at the time we were just using Swipe, which was less secure than what we have now. What I started to see over time is an uptick steadily in the number of security incidents and the scale. So the first time I handled a ransomware matter was probably in 2013-2014, and at that time, these were pretty amateurish groups. They were encrypting, you know, maybe part of someone's system, the company's systems, and then demanding between like $5,000 and $50,000 to get the decryption key. They weren't doing data exfiltration.

So companies, as they increasingly were targeted by ransomware attacks, got smarter about their backup strategy. And so when you -- I always explain it this way, but it's an imperfect analogy, so

bear with me. So picture you have a house and somebody comes, a bad guy comes and padlocks the outside of your house; you can't get in. That's essentially what the encryption feature is of a ransomware attack. Now, let's assume every few hours, you make a shadow copy of your house, and it's next door, and if the shadow copy is not encrypted because you have put in measures -- put measures in place to separate your shadow copy from your existing house, you would be able to then just move into the second house, and maybe you lose a little bit of the data from the last few hours since the last backup, but you could move over.

And so companies started to outsmart the threat actors because they were deploying these backup strategies that enabled them to not have to pay a ransom.

So we really saw a new tactic around the time of COVID, and this was threat actors taking advantage of the rapid shift to remote work, where they were coming in and exfiltrating large volumes of data.

Now, at the time, when I say large volumes, I'm talking 30, 40, 50,000 files. And so they would extort you in two ways. One, you've got the encryption piece, but you might not need the decryption key because you've got your backup house, right, or your backup data. Or they would say, "Well, if you don't pay us, we're going to take this data that we stole and we're going to post it on the dark web on our site with your name so that everybody is aware that this happened to you and their information is now out there."

What we have seen in the last two or three years are a few trends that are frankly extremely concerning. Trend number one is the exfiltration of massive quantities of data. So 13 terabytes, which was what was affected here in terms of exfiltration, that would have been unheard of three years ago, and now I have several matters where we're in the terabytes of data that have been exfiltrated, and they're usually exfiltrated from a Data Lake or some sort of -- what I call an

unstructured dataset, meaning they're not getting into your database and taking things from your database because that's a lot of trouble. That could tip you off that they're in your systems. Instead, they're going for what they consider to be more accessible, which is the Data Lake information, and they're stealing that information and removing it.

When you have that quantity of information and you're trying to figure out what's in it, I think here it was over 3 million files. I mean, that is an incredibly large amount of information. So trying to figure that out with any degree of certainty is really difficult. It's really time consuming. Now, add that to all the other operational issues that are caused by an encryption event, particularly when you are providing a crucial service that impacts public safety.

And so my opinion in this report about the speed and the way that Nova Scotia Power made these notifications, all three rounds, is based in that context

of having a real experienced understanding of exactly what happens in these incidents and how difficult it is to get it right.

I have what's becoming kind of a tired saying, but I always say in a large incident, when you're responding as a victim company, you're often choosing the best bad option. And by that, I mean when you look at your options for whatever decision point you have to make, there is a downside to every single one of those options. There is no perfection.

[4:10:09] And so through that lens as well, looking at the response of Nova Scotia Power, what I see is a company that took this really seriously. They were raising awareness, not only of the issues around the encryption and the service issues, but also about the fact that customer information was potentially affected, and they knew it relatively early, and they were taking steps to inform the public and make sure they had the support in place.

I realize that was probably more than you asked for, so hopefully that was helpful though.

Q. I was worried that Mr. Clarke was going to object that you're going beyond the opinions in the report, but I'll get to that part of the evidence.

We'll move on. Let's talk about -- you responded to a question from Mr. MacLeod. So it's with respect to the five-year timeframe.

A. Yeah.

Q. And if I understood the evidence correctly, I think you said that the risk of the use of that information dissipates over time. I'm not sure that's what you meant, but is that what you meant?

A. The risk of the misuse of that information, as it relates to a particular incident, as opposed to any other misuse of the information, typically dissipates over time. So ---

Q. Let me stop you there. Is it the risk that dissipates with an incident or the fact that you

can't associate it with the incident that dissipates?

A. It's a good distinction. So let me take a step back and maybe explain it a little bit better.

When your data is posted on the shame site, which is what we call the Dark Web site of these criminal groups, and when you don't pay a ransom, that is where the data ends up. One fortunate thing is now that these threat actors are stealing such large quantities of information, they can't really host. It's your data and it's every other victim company who didn't pay. They can't really host that size of data for very long because it's expensive. It's also clunky and difficult to download. So what happens over time, within two or three months, the data gets removed off of the site by the threat actor because they have moved on and replaced you with new victims. And then from that point in time, the less available the data is, the less likely it is to be sold, misused, et cetera.

A Social Insurance Number, which in the United States, where I said is the equivalent of our social security number, that is a static number, and obviously it's a concern. My point was that the longer time goes on, the likelihood that a risk to that number will be a result of the -- that one particular security incident dissipates.

I think you would be surprised that your information's probably far more out there than you realize.

And so when we deal with handling, in particular class action lawsuits, the question that always comes up is even if someone says, "I believe someone misused my information and tried to", for example, "take out a loan in my name", it's very difficult to tie that activity to a particular breach because of just the nature of this information.

And those are just reportable breaches. I think there's a lot of companies who don't

know they were breached or if they have reported it, who I think are the source of some of the leak of this information.

Q. Okay. And just a question on -- there was an answer with respect to the counsel for Mr. MacLeod with respect to the issue of individual security clearances. And my assumption, although perhaps it's a wrong one, but security clearances in the United States, I would have assumed because of the role the United States plays in many, many, many different parts of the world, would be a very important aspect of privacy breaches.

Have you had experience with that type of situation, where ---

A. Very minimal.

Q. --- people lose their clearances because their privacy was breached?

A. Very minimal. I have handled breaches for defence contractors, where part of the

information exposed was the security clearance level of certain people who either worked for or had affiliations with that organization.

Q. So you don't have any experience with having different types of monitoring depending on what your security clearance is?

A. We would typically not recommend to our clients to have different monitoring offerings for different people, different circumstances. If you're dealing with a security clearance issue, at least in the United States, and I can't speak to Canada, you know, there may be mechanisms through the Department of Defence, which I guess we're calling the Department of War now, or other government agencies to try to obtain some sort of additional protection. Although, you know, candidly, our multiple government agencies in the United States have had massive breaches, including breaches of security clearance information, and those are the ones that are reported. So I wouldn't treat anyone differently if there's not a

particular legal reason to do so.

And keep in mind too, what credit monitoring is intended to do is not provide a complete, you know, protection for all potential risks to an individual. And so I'm not sure that offering longer credit monitoring to someone because they carry a government security clearance actually does anything to address any, you know, potential risk of harm to those individuals from the exposure of their clearance information.

Q. Okay.

MEMBER MELANSON: Thank you. Those are my questions.

VICE CHAIR DEVEAU: No questions.

THE CHAIR: Mr. Norwood, if we can go to the previous page, please, in that exhibit. Looking at line 4. Sorry, could you scroll to the bottom, please? I'm not sure this is the right page. Yeah, okay.

Just bear with me for a second.

Sorry. Sorry, Mr. Norwood. It's page 74, line 5.

QUESTIONS FROM THE CHAIR

Q. Ms. Valdetero, the statement in your evidence there says, "The record establishes that this was not a routine data breach." And I just had a couple of questions arising from that. First being, what do you consider to be a routine data breach?

A. So a routine data breach to me is one that is limited in scope. So it typically involves the breach of a single user account or a single user email account with limited impact on potential data access or data exfiltration that could require notification to individuals and regulators.

Q. Okay. And in terms of the thousands of incidents that you have dealt with, I would take it most would not fall into that routine classification as you've just described it?

A. Correct.

Q. On the spectrum of significance in terms of security incidents that you've dealt with in

terms of volume of data exfiltrated, the number of customers impacted, where would this one sort of fit in the spectrum of matters that you've dealt with?

A. Probably top 10 to 15 percent.

Q. Top 10 to 15 percent. And have you been involved in data breach incidents involving regulated utilities providing monopoly service?

A. Yes. I think I was already asked that maybe a little bit earlier.

Q. Okay. I wasn't sure if that was just in terms of your general advice to companies or if you were actually involved in data breaches with those.

A. I was involved in multiple data breaches.

Q. Okay.

A. Yeah, for the same entity.

Q. Okay. And in terms of those, how many involved the loss of information for nearly a million people?

A. For that particular entity?

Q. Yeah.

A. None.

THE CHAIR: Mr. Norwood, if we could turn to Ms. Ralph's evidence for a moment, please, Exhibit N-14. I didn't note the page number, but it's paragraph 55 that I'm looking for.

BY THE CHAIR:

[4:20:13] **Q.** So I want to draw your attention to -- it's a sentence that begins partway through that paragraph, about halfway:

> In light of this, a cautionary approach would have been to explain to customers that since it could not determine with specificity which data points were accessed by the threat actor, customers should assume that all data points were accessed, as opposed to NSPI simply saying they could not determine specificity.

You disagreed with this, and I just want to better understand why. I think part of what you said, if we can flip back to your evidence at N-17, page 82, and you can take a look at it, but I'm focussing

on your comment that:

> It may cause unnecessary alarm among customers whose data was not, in fact, meaningfully compromised.

A. Yes. Sorry, would you like me to explain that a little bit more?

Q. Please, yes.

A. Okay. All right.

So this goes back to my comment earlier about you're often choosing the best bad option. So in an ideal world, you would have no impediment to be able to determine exactly who was affected, exactly what about them was affected, and get notices sent directly to those people at current addresses. Right?

Here, they were trying to notify the -- at least the 277, I'll start with that -- the 277 folks as quickly as possible, and they did that within about 18 days, which is really, really fast.

When you are trying to pick the best bad option, which is speed over precision, it is very

difficult to say this is what is -- has been affected about each person with certainty, with specificity. It's extremely difficult, and very few companies actually are able to accomplish that, and when they are it's only because it's in a structured dataset and it's all pretty similar across every individual who is getting a letter.

Here, my understanding is that some of the information for individuals was a little bit less sensitive. So you know, your -- and I know it's all in the eye of beholder, and I'm a little jaded -- but contact information, your home address, that type of thing. Some of it was a bit more sensitive, obviously, you know. So for the Social Insurance Number folks, yes, it's clearly an area of concern, and then I think there were some driver's licence and some bank account people.

I think it would be misleading to tell them they should assume all of that information has been impacted when we actually don't know that it was, and it's almost kind of offering advice that goes beyond, I think,

what's appropriate for a company making a notification like this to be offering under the circumstances.

You know, like I said, ideally they would have been able to provide more specificity, but I would not have taken this approach that's suggested by Ms. Ralph, and it's not customary to do so in the industry.

Q. And why do you feel customers would be unnecessarily alarmed by taking the approach that Ms. Ralph suggested versus what actually happened in this case?

A. I think if you're telling someone "We don't know, but you should assume it's everything we could potentially have about you", that to me has a scarier message than, "Here's what happened. It may have included some or all of the following," which is very standard language, and which is what a lot of companies use.

So in terms of were they following

industry standard practices for the approach under the circumstances? They are.

Ms. Ralph's recommendation is not typical and it's not industry standard. So I'm not surprised they didn't do that.

Q. Okay. And later on in the paragraph, you make a comment about it potentially creating, "...an inaccurate impression of the scope of the breach." Could you elaborate on that?

A. That kind of goes back to my testimony just now, is if you're telling someone, "Assume it's all affected," then to me there's very little difference between that and telling someone, "All of this is affected." And I think that goes too far, based on what they knew at the time.

Q. And the phrase you use sort of four lines down, "Meaningfully compromised," I think that may go back to what you mentioned a moment ago in terms of the type of information that was taken, whether it's a

email address or versus a SIN number?

A. Yes, exactly. Or the fact that maybe their information wasn't compromised at all. My understanding is they didn't really have confirmation at this time. They had reasonable belief, they didn't have confirmation.

And that's another piece that you're always dealing with when you're trying to make notifications quickly, is you may have a sense, but if your forensic investigation is ongoing, for example, facts change. And people are always surprised about this, but what clients call me and tell me they think is going on Day 1 of an incident is often pretty different from what we figure out on Day 14 or Day 21, after we have had a forensic investigator come and complete their investigation. And for a breach of this scale, that's particularly true.

Q. Okay, those are my questions. Thank you very much.

THE CHAIR: Are there anything arising from Board Panel questions?

--- (No response)

THE CHAIR: Not seeing any.

Anything by way of re-direct?

MR. CLARKE: No, Mr. Chair.

THE CHAIR: Ms. Valdetero, thank you very much for your evidence and your participation in this proceeding.

MS. VALDETERO: My pleasure. Thank you.

THE CHAIR: All right. You're clear to go. Thank you.

MS. VALDETERO: Thank you.

(WITNESS WITHDRAWS)

THE CHAIR: Okay. So 4:30 now, so I think we'll break for the day. We'll resume tomorrow with the Consumer Advocate's witness, and we'll proceed with Ms. Ralph after that.

Anything before we wrap?

--- (No response)

THE CHAIR: Okay. Have a good evening, everyone. We'll see you in the morning at 9 o'clock.

--- Upon adjourning at 4:26 p.m.

CERTIFICATE OF COURT TRANSCRIBER

I, Patricia Cantle, hereby certify that I have transcribed the foregoing, and it is a true and accurate transcript of the evidence given in this matter, M12600.

Patricia Cantle
Registration No. 2017-001
ICDR, ICDT
Certificate No. IAPRT-2142

Halifax, Nova Scotia
Wednesday, August 19, 2026